SPAWAR
Systems Center
San Diego

TECHNICAL DOCUMENT 3100
January 2000

Commercial Off-the-Shelf (COTS) Security Products Evaluation Process

J. Yen

Approved for public release;
distribution is unlimited.

SSC San Diego

DTIC QUALITY INSPECTED 1

20000218 059

TECHNICAL DOCUMENT 3100
January 2000

Commercial Off-the-Shelf (COTS) Security Products Evaluation Process

J. Yen

Approved for public release;
distribution is unlimited.

SPAWAR
Systems Center
San Diego

SSC San Diego
San Diego, CA 92152–5001

SSC SAN DIEGO
San Diego, California 92152–5001

E. L. Valdes, CAPT, USN
Commanding Officer

R. C. Kolb
Executive Director

ADMINISTRATIVE INFORMATION

This document was prepared for Space and Naval Warfare Systems Command (PMW 161) by the Information Assurance Network Security Branch (D872), SSC San Diego.

Released by
J. L. Alvarez, Head
Information Assurance
Network Security Branch

Under authority of
E. A. Engh, Head
Information Assurance
& Engineering Division

SB

EXECUTIVE SUMMARY

This document is the first in a series of documents that will define a formalized process for evaluating commercial off-the-shelf (COTS) network security products in support of Space and Naval Warfare Systems Command (SPAWAR) PMW161. Further dissemination to other Navy and Department of Defense (DoD) activities is encouraged.

The objective is to develop a generic process for evaluating COTS network software security products. This process will:

- Evolve with changing conditions.
- Be adaptable to future evaluations.
- Foster cooperative relationships with COTS product vendors and other government COTS product evaluation efforts.
- Assess suitability for inclusion of a product into the Navy/Marine Corps Intranet (N/MCI) and Information Technology Service Center (ITSC) architectures.
- Lead to the development of security assessment criteria.
- Include security assessment and verification.

This document describes the COTS security product evaluation process, defines the seven phases of the evaluation process, outlines the documentation requirements of the process, and discusses how the evaluation process fits into the overall evaluation framework. The evaluation process as described in this document is expected to be revised as the overall evaluation framework is developed. Appendix A contains additional information regarding Common Criteria and protection profiles and Appendix B contains additional details regarding the Information Assurance & Engineering Division (D87) formal inspection process.

CONTENTS

APPENDICES

Figures

Tables

1. INTRODUCTION

This document is the first in a series of documents that will define a formalized process for evaluating commercial off-the-shelf (COTS) network security products in support of Space and Naval Warfare Systems Command (SPAWAR) PMW161. Further dissemination to other Navy and Department of Defense (DoD) activities is encouraged.

1.1 OBJECTIVES

Develop a generic process for evaluating COTS network software security products. This process will:

- Evolve with changing conditions.
- Be adaptable to future evaluations.
- Foster cooperative relationships with COTS product vendors and other government COTS product evaluation efforts.
- Assess suitability for inclusion of a product into the Navy/Marine Corps Intranet (N/MCI) and Information Technology Service Center (ITSC) architectures.
- Lead to the development of security assessment criteria.
- Include security assessment and verification.

1.2 POINTS OF CONTACT

Table 1 lists personnel who contributed to the development of this document.

Table 1. Points of contact.

Name	Role	Phone	Email
Scott Henderson	Sponsor (PMW161-2)	(619) 524-7507	henderss@spawar.navy.mil
Mike Harrison	D872 Branch Head	(619) 553-9440	msh@spawar.navy.mil
John Yen	Editor	(619) 553-9404	yen@spawar.navy.mil
Jorge Alvarez	System Security Engineer	(619) 553-9421	jalvarez@spawar.navy.mil
Guy Casciola	INFOSEC Analyst	(619) 553-1145	casciola@spawar.navy.mil
Sylvia Davis	Software Quality Assurance	(619) 553-9418	sdavis@spawar.navy.mil
Bob Franco	Secure Voice	(619) 553-9429	franco@spawar.navy.mil
Nate Kunes	System Security Engineer	(619) 553-7134	kunes@spawar.navy.mil
Chris McAllister	Software Engineer	(619) 553-5178	cmcallis@spawar.navy.mil
Jorge Pena	System Security Engineer	(619) 553-7134	penaj@spawar.navy.mil
John Townsend	Business Manager	(619) 553-1382	townsend@spawar.navy.mil
Steve Turner	Secure Voice	(619) 553-7860	st108@spawar.navy.mil

1.3 SCOPE

This document describes the COTS security product evaluation process, defines the seven phases of the evaluation process, outlines the documentation requirements of the process, and discusses how the evaluation process fits into the overall evaluation framework. The evaluation process described in this document is expected to be revised as the overall evaluation framework develops.

Appendix A contains additional information regarding Common Criteria and protection profiles.

Appendix B contains additional details regarding the Information Assurance & Engineering Division (D87) formal inspection process.

Appendix C contains additional details concerning the Security Proof of Concept Keystone (SPOCK) program's evaluation process.

1.4 GOVERNMENT OFF-THE-SHELF (GOTS) PRODUCTS

The process outlined here can also be applied to evaluations of government off-the-shelf (GOTS) or other non-developmental item (NDI) security products.

2. BACKGROUND

With network security technology evolving rapidly, it is nearly impossible to develop and deploy network security products using traditional Department of Defense (DoD) acquisition processes. Also, the globalization of the information infrastructure has driven private industry to develop security products for the commercial market. Therefore, the Navy can leverage selected COTS security products to support some of its network security needs.

2.1 RATIONALE

Given the task to evaluate and determine which CO ΓS network security tools and freeware tools provide quality information security solutions to a Navy network, it is necessary to formalize a process under which network security product evaluations can be performed consistently.

To compare products, COTS network security products must be categorized in accordance with specific functionality (such as firewalls and audit tools) and tested with respect to Navy-applicable security requirements. No formal process exists for establishing applicable security requirements or categorizing and evaluating network security products among the activities evaluating COTS products forthe Navy.

2.2 FRAMEWORK

The increased use of COTS and NDI implies that a different set of skills is needed to deal with COTS/NDI systems in contrast to traditional DoD-unique systems. With the current emphasis on COTS acquisitions, the Information Assurance & Engineering Division (D87) is taking a leadership role in these acquisitions, including defining a new type of program agent, the Life Cycle Management Agent (LCMA). Therefore, Space and Naval Warfare (SPAWAR) Systems Center, San Diego (SSC San Diego) D87 has developed strategies and techniques for acquiring and supporting COTS-based systems.

SSC San Diego D87 has formalized the D87 Process Framework (see figure 1) for performing system security engineering and determining solutions. This process can be useful in fostering a consistent methodology among the activities supporting COTS security product evaluations.

The D87 Process Framework is an iterative process that can start at any point and can be taken through as many cycles as needed. Process components include the following:

- The concept of operations (CONOPS) that defines the fleet operations need and the system that will satisfy the need.
- Gathering of technical information, such as technical reports, product information, and minutes of meetings/conferences/workshops.
- Analysis of available information on products.
- System engineering that results in a system design.
- Assembly of possible solutions and their costs.
- Field tests that demonstrate the technology.

- Evaluation that integrates inputs from the users as well as the developers.

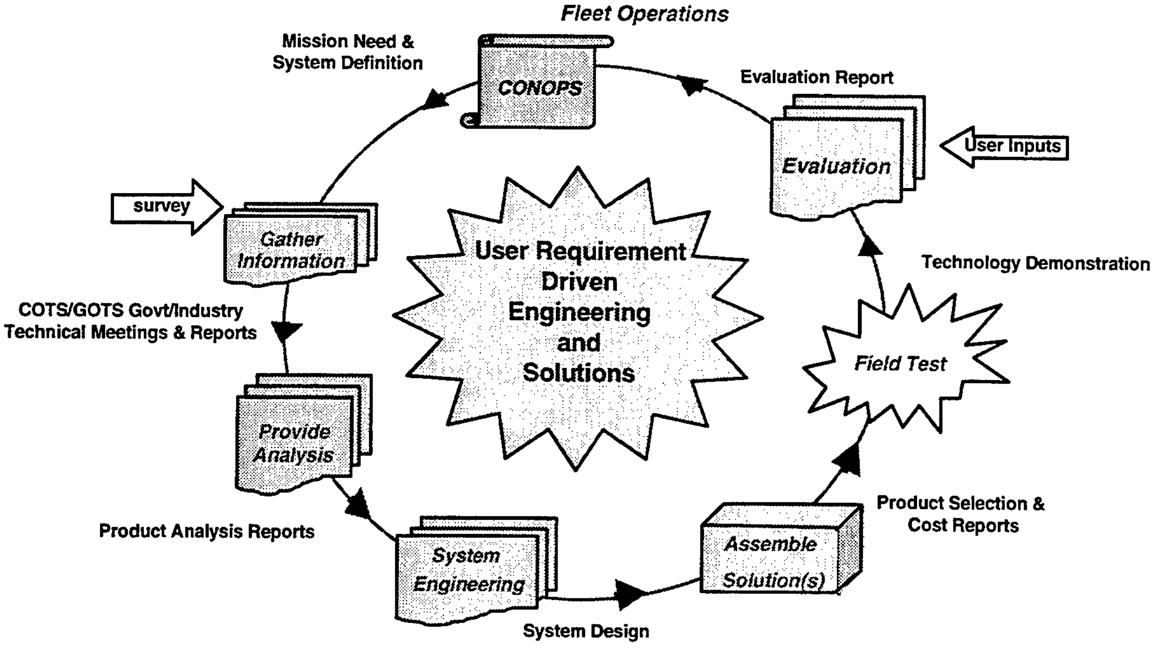


Figure 1. D87 process framework.

2.2.1 Evaluation Report

An important output of the D87 Process Framework is the evaluation report that incorporates user inputs. This report provides gap analysis, risk management, and requirements feedback to the developers. A gap analysis looks at the gap between need and what is really available, and then recommends how to bridge the gap.

2.2.2 References

References for SSC San Diego D87 processes include the following:

- J. H. Townsend. 1996. "The Real NDI Buyer's Guide." Technical Document 2911 (Jun). Naval Command, Control & Ocean Surveillance Center RDT&E Division,[1] San Diego, CA.

- *SPAWAR Systems Center San Diego (SSC SD) Communications and INFOSEC System Support and Integration Division Code D87 Business Plan, FY 99.*[2]

Figure 1 is adapted from the SSC San Diego D87 Division Overview.

[1] Now SSC San Diego.

[2] Available on a case-by-case basis. Submit request to C.O. SPAWARSYSCEN SAN DIEGO, Attn: D87.

2.3 METHODOLOGY

The COTS Product Evaluation Framework (see figure 2) is adapted from the D87 process framework. The mission need drives the security aspects of the system CONOPS. The security CONOPS (SECONOPS) is a subset of the system CONOPS that drives the security policy and the security requirements. The security product category determines the protection profile(s) used for this evaluation. The product category information and the security requirements then form the security profile, as defined by the D87 process, for the security product evaluation process. Finally, evaluation process results feed back into the mission need through changes to SECONOPS and the N/MCI and ITSC architectures.

The primary driving force in applying this methodology is that it supports modern systems engineering techniques such as the spiral and rapid prototyping methods. The spiral model is an iterative process with four quadrants (planning, risk analysis, engineering, and customer evaluation), where each software version goes through new planning, risk analysis, engineering, and customer evaluation phases. Rapid prototyping is a process that develops a first, quick version of a product and provides immediate feedback from the user.

In most current COTS applications, the product is often available before the complete development of the CONOPS or SECONOPS, which leads to an earlier capability, but usually results in an incomplete mapping of needs to solutions. Therefore, the process must be iterative.

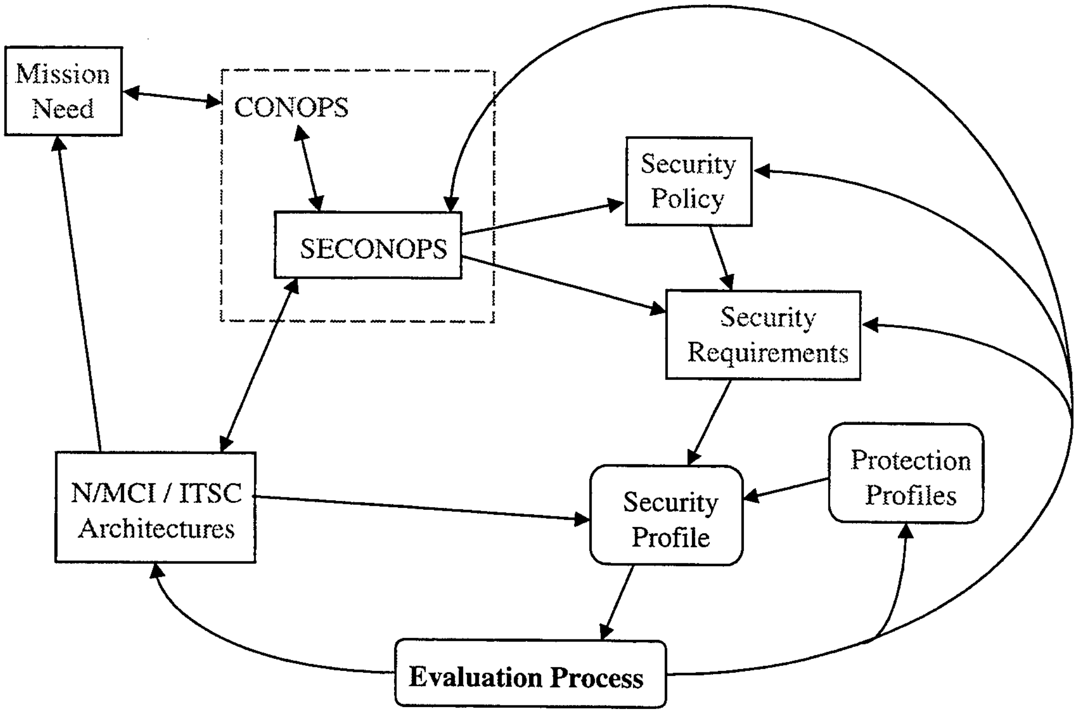


Figure 2. COTS product evaluation framework.

2.3.1 Security Profile

D87 will formalize a security profile development process for a network security product, including a product categorization methodology and evaluation criteria (protection profiles) development process. This security profile process is the precursor to the evaluation process and will be documented in a separate document. It is expected that this security profile document will incorporate an incremental approach to security assurance that is consistent with the technological advances made in both the commercial and Government communities.

The results of the evaluation process will be fed into N/MCI and ITSC architectures. Any resultant architectural changes will then feed back into the mission need and restart the cycle. Evaluation process results will also affect the SECONOPS, CONOPS, security policy, and security requirements, which in turn impact the mission need.

2.3.2 Product Category

Security products must be categorized into generic groups (such as firewalls and audit tools) so that similar products can be evaluated in a common framework where comparisons of evaluation results are valid. Categorization will be detailed in the security profile document.

Categories are based on product features, threats countered, and protections provided. The product categorization will initially be based on commercial certification processes, Common Criteria protection profiles, Trusted Product Evaluation Program (TPEP) rating, National Information Assurance Partnership (NIAP) protection profiles, Defense Information Assurance Program (DIAP) protection profiles, and current customer satisfaction.

2.3.2.1 Common Criteria. Future product categories will be based on the Common Criteria (see Appendix A for more details) because that will be the standard of security evaluations. General and specific criteria for each product category will be defined as a security profile, which may include Common Criteria protection profiles. Security profiles will be developed for each product category evaluated, and will be covered in the security profile document.

2.3.2.2 Passing Criteria. Products must be evaluated by both general and specific criteria, depending on the category. The passing criteria are a subset of the evaluation criteria and will be discussed in the security profile document. Below are some examples of passing criteria:

- Does the product meet the Navy's minimal performance criteria?
- Does the product meet the vendor-stated performance criteria?
- Is the product sufficiently user-friendly?
- Does the product meet the relevant security standards?
- Does the product satisfy the system CONOPS and SECONOPS?
- For any defect, is the vendor willing to bring the product up to a defined standard?
- Is the vendor willing to provide upgrades in response to new security threats?

2.4 PROCESS OVERVIEW

As figure 3 shows, the COTS security product evaluation process of figure 2 currently contains seven phases.

In figure 3, the boxes with question marks (?) are decision points during the evaluation process and are described in the following sections. Note that while these phases are shown as consecutive and distinct, some phases often are conducted in parallel. In theory, the process can start at any phase as long as it propagates through all phases to complete at least one cycle. Also note that this process is an idealization which can, and should, be modified as circumstances dictate, as befitting a living process.

An obvious example of straying from the above process is that often the Contact phase may begin the process with a call from the vendor, so that the Research phase follows the Contact phase and runs concurrently.

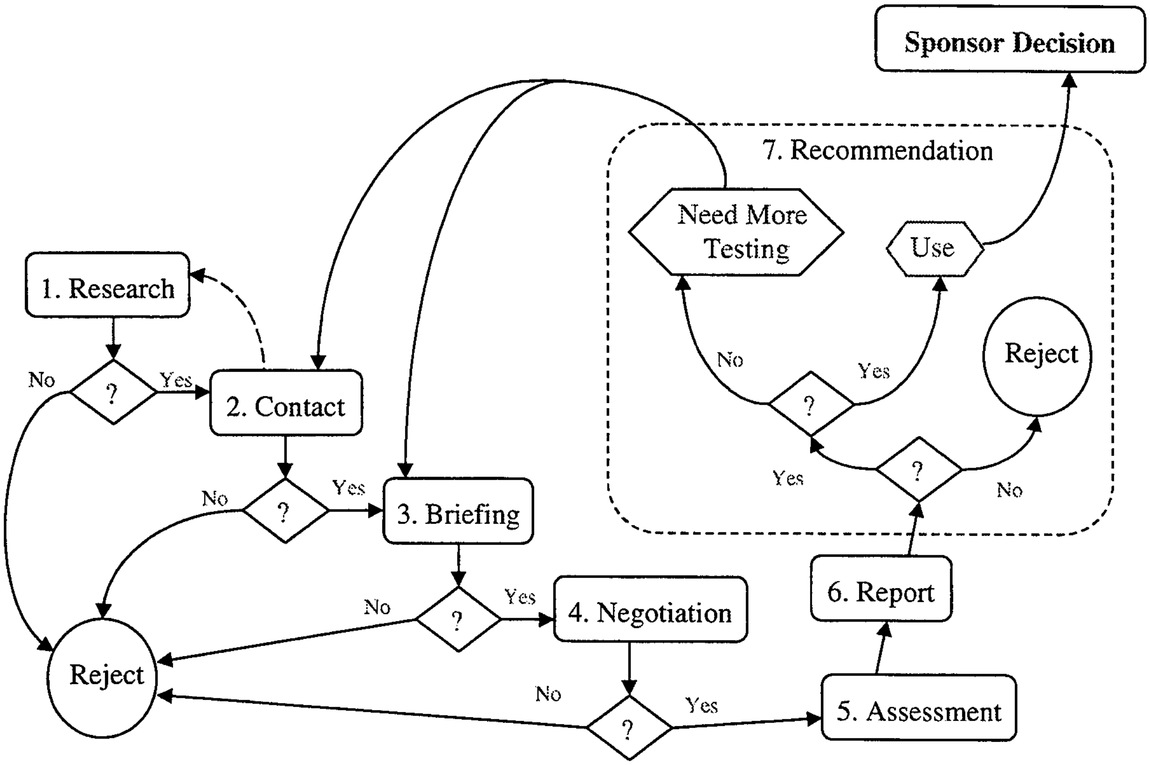


Figure 3. Evaluation process overview.

3. PRELIMINARY PHASES

The first four phases (Research, Contact, Briefing, and Negotiation) of the process are grouped as "preliminary" to the three "evaluation" phases (Assessment, Report, and Recommendation).

3.1 RESEARCH PHASE

The first phase involves researching the product and the vendor, although the process may start with contact from the product vendor. Figure 4 illustrates this phase. Combining the various blocks representing information will determine whether the product fits a Navy need.

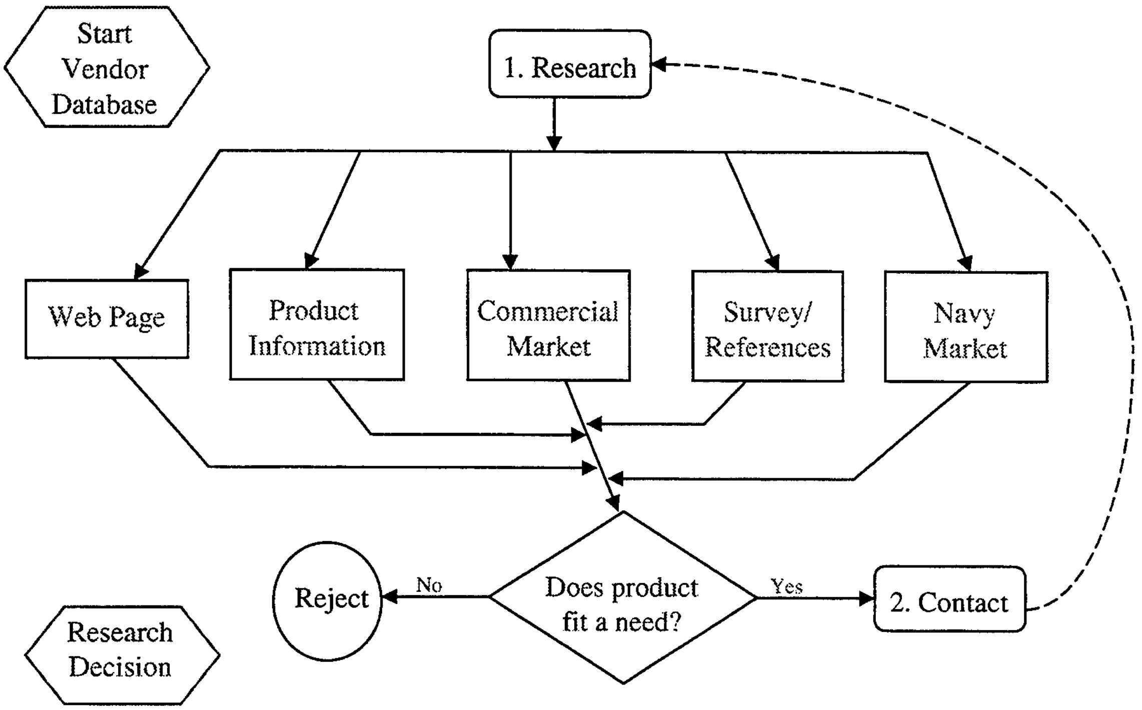


Figure 4. Research product/vendor.

3.1.1 Information Sources

Initial information can be obtained from the vendor's web page, which may contain product brochures, fact sheets, and related documents. Professional publications from both Government and industry can provide useful information regarding the product. Finally, another useful information source is other companies with competing products.

3.1.2 Targeted Information

Some of the vendor/product information to look for are product specifications, the vendor's market position (product longevity depends on this), past customers, product performance history, and any security evaluation process that the product has underwent.

3.1.3 Survey and References

Other Government activities (such as the National Security Agency [NSA], Defense Information Systems Agency [DISA], and Naval Research Laboratory [NRL]) and companies that have used or evaluated the product previously can be surveyed for information. Table 2 is a sample survey questionnaire sent to Government activities or companies to elicit information regarding the product.

Table 2. Sample survey questionnaire.

Concept of Operations	Provide information regarding how the product is used.
Product Security	Provide available information regarding host security features that are in turn supported by the product.
Security Assurance	Answer whether the host systems have previously been evaluated for security. Some acceptable product assurance evaluation processes are: • Trusted Product Evaluation Program (TPEP) • Federal Information Processing Standards (FIPS) 140-1 • National Information Assurance Partnership (NIAP) • Defense Information Assurance Program (DIAP) • Common Criteria • Security Proof of Concept Keystone (SPOCK)
Product Performance	Provide information regarding performance of the product.
Product Scalability	Provide information regarding scalability of the product.
Product Cost	Provide the cost of deploying the product, such as installation, training, and maintenance.
Company Information	Provide available information on the following: • Company health • Capability of developers • Product support reputation

3.1.4 Navy Market

Identify the size of the potential Navy and/or DoD market. This information is needed to determine whether Navy/DoD is a significant market in itself (and thereby able to influence market standards and practices).

3.2 CONTACT PHASE

The second phase (see figure 5) involves communication with the product vendor. In this phase, information will be collected and personal contacts established. The information collected and a possible site visit determine whether the product vendor should be invited to make a product briefing. Note that the process can start with contact from the vendor and then proceed to the Research phase.

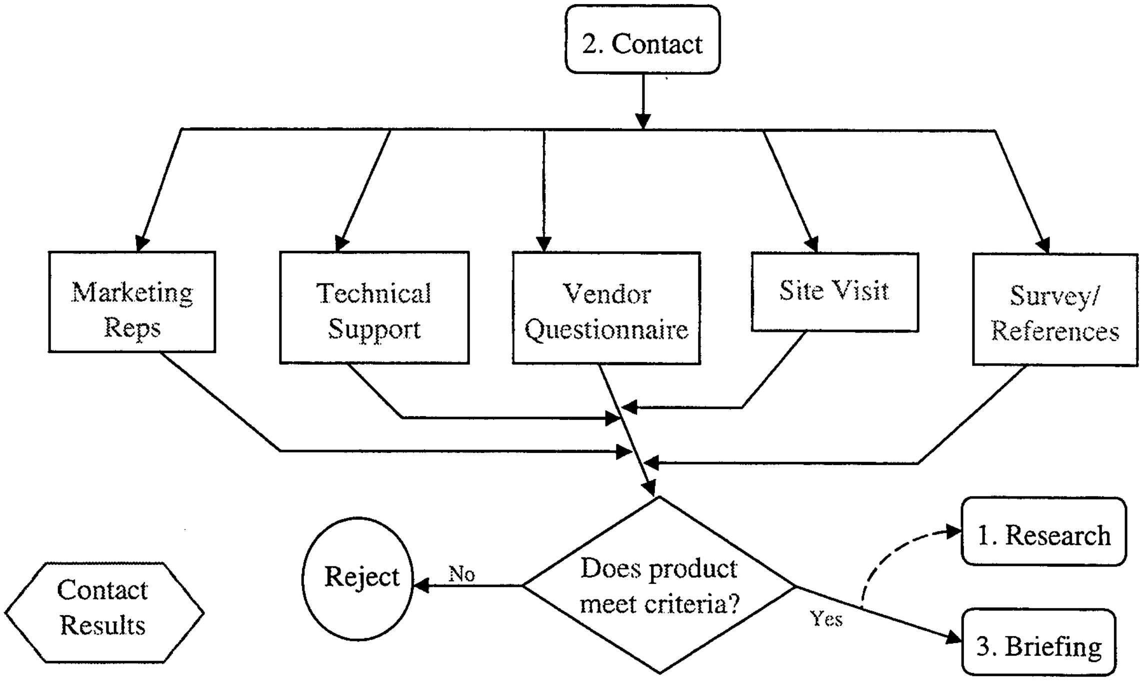


Figure 5. Contact vendor.

3.2.1 Marketing Representatives

The usual first points of contact are in the vendor's marketing office, which usually means dealing with people focused on sales rather than in-depth technical knowledge. This is still a good starting point to reach the desired people in the vendor's organization.

3.2.2 Technical Support

Technical support people, when available, are generally the best sources of technical information needed for understanding the product. However, they are usually reached only after contacting the marketing people.

3.2.3 Vendor Questionnaire

The vendor will be asked to supply the Government with any available information regarding the product. A vendor should, in theory, be invited to brief his product only after completing and returning a vendor questionnaire. However, that may be somewhat impractical, as the Government does not always have sufficient influence with industry to enforce compliance.

Table 3 shows a sample vendor questionnaire. It is not expected that all the questions can be answered, but the vendor should be encouraged to provide available information. Some of these questions may be difficult to answer and are included to elicit points of contact, such as the question regarding performance. The vendor responses will be compared against other vendors' responses and the relevant security requirements.

Table 3. Sample vendor questionnaire.

Concept Of Operations	Provide available product concept of operations (CONOPS) or security CONOPS (SECONOPS). Equivalent commercial product support documentation regarding how the product is used is acceptable.
Product Security	Provide available information regarding security features supported by the product.
Security Assurance	Answer whether the product has previously been evaluated for security. Some acceptable product assurance evaluation processes are: • Trusted Product Evaluation Program (TPEP) • Federal Information Processing Standards (FIPS) 140-1 • National Information Assurance Partnership (NIAP) • Defense Information Assurance Program (DIAP) • Common Criteria • Security Proof Of Concept Keystone (SPOCK)
Product Performance	Provide references of previous efforts to demonstrate performance, both functionalities and usability. The main questions are what environments the product has been used in and whether the product performed as advertised.
Product Scalability	Provide references of previous large-scale efforts to demonstrate scalability. The main question is whether the product can support the whole Navy without overloading.
Product Cost	Provide the per unit cost of the product. Volume discounts, annual license costs, maintenance support costs, and other information are of interest.
Market Position	Provide information regarding the market position and share of each product. Also of interest will be long-term vendor plans for that product, such as support strategy and size of support staff.
Company Information	Provide available information on the following: • Company size and assets • Number of developers • Financial stability • Investors market capitalization

3.2.4 Site Visit

If possible, visit the vendor site. Such a visit can provide nontechnical information regarding the vendor, such as how the company is performing, professionalism within the company, and personnel morale.

3.2.5 Questionnaires Review

Results from the questionnaires sent to the vendor and relevant activities are reviewed. Based on a review of questionnaires, a tentative conclusion can be reached regarding whether the product satisfies some Navy need.

3.2.6 Invitation to Briefing

If the product has the potential to satisfy Navy needs, then invite the vendor to give a presentation regarding the product of interest. A face-to-face meeting is usually best to get an idea of whether the product is really useful. An added benefit of a product briefing is the education of other Government personnel regarding the product.

A clear agenda should be worked out in advance with the vendor. Also stress to the vendor that technical personnel are also invited to provide substance to the briefing.

3.3 BRIEFING PHASE

The vendor will provide a presentation regarding the product and possibly a demonstration (see figure 6). To encourage the vendor to demonstrate the product, equipment should be made available for temporary use during the visit.

The Government's objective during this phase is three-fold:

- Establish vendor points of contact.
- Elicit as much technical information regarding the product as possible.
- Determine whether the evaluation process should proceed.

The vendor's marketing people tend to gloss over technical details in favor of sales pitches. Therefore, before the presentation, emphasize the technical nature of the audience and the technical questions (related to the questionnaire) likely to be asked.

After the presentation and demonstration, both the Government and vendor representatives will question each other regarding intentions and resources to determine whether an assessment is practical.

3.3.1 Navy Questions

The Navy must determine whether the product can potentially satisfy a Navy need. If so, it must then determine whether the need is sufficient for the Navy to commit resources to effectively test the product.

3.3.2 Product Retooling

If the product does not satisfy a Navy need, then the vendor has the option to retool the product to satisfy the need. The vendor can then give another brief describing the changes.

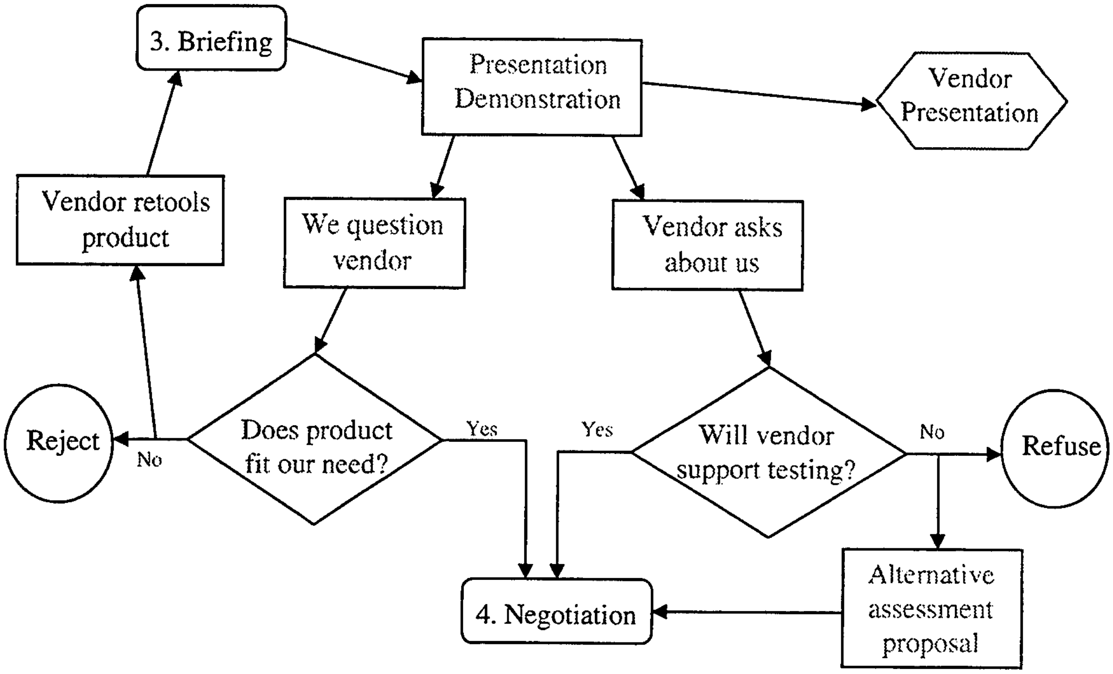


Figure 6. Vendor briefing/demonstration.

3.3.3 Vendor Questions

The vendor must determine whether the Navy fits the vendor's business plan. If yes, then they must develop a business case for supporting the test as a cost-effective and worthwhile investment and convince their management of the case.

3.3.4 Alternative Assessment

Even if the vendor does not want to support a free evaluation, an alternative assessment plan may be negotiated and implemented (see section 4.1.2). Such an alternative can be pursued if the Navy decides that the need is great and the product best fits the need. In this case, the Navy is expected to contribute the resources needed for the evaluation.

3.4 NEGOTIATION PHASE

If both the Government and the vendor decide to proceed with an evaluation, then they will negotiate the terms of the assessment. Figure 7 shows some of the negotiation subjects that must be agreed on before an agreement is reached.

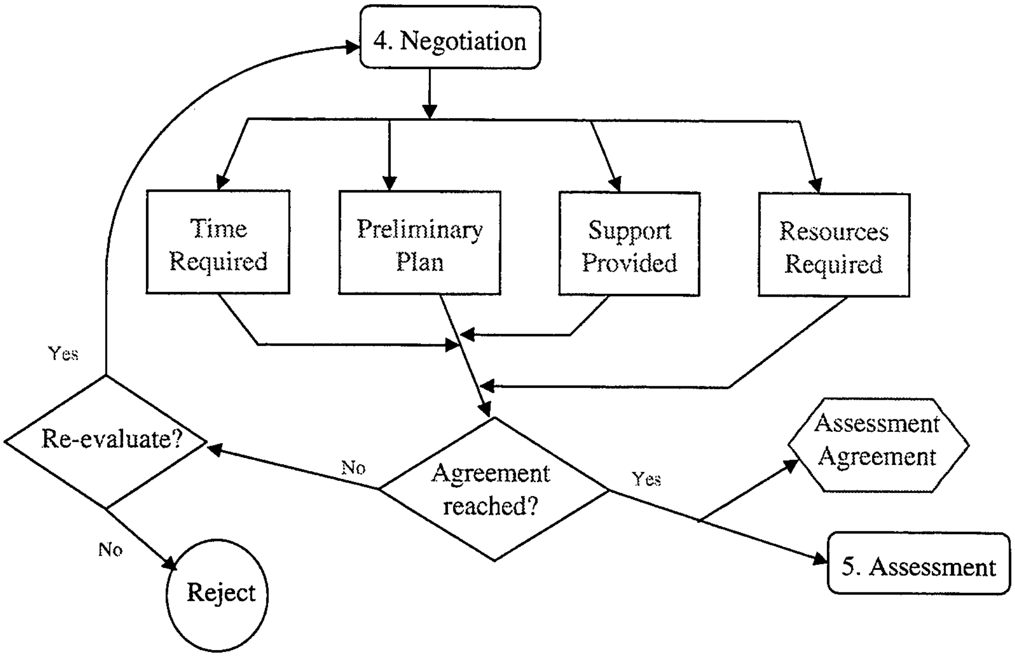


Figure 7. Negotiate testing.

3.4.1 Process

The first decision is which product(s) will be assessed, for what period, and the requirements under which the assessment will be performed. An evaluation process should be agreed upon, resulting in a preliminary plan that will be expanded into the test plan for the assessment. This plan shall include vendor technical claims that the Government and the vendor agree to evaluate during the assessment phase.

3.4.2 Vendor Support

A major question is what support the vendor is willing to provide, such as product training for Government testers and technical support during the test period to answer questions.

3.4.3 Government Resources

The Government must determine whether the personnel, equipment, and facilities needed for the evaluation are available.

3.4.4 Re-Evaluation

If an agreement is not reached, then both the Government and the vendor must re-evaluate their positions. If appropriate, re-enter negotiation.

3.4.5 Assessment Agreement

The assessment agreement is made when the Government and the vendor decide to proceed with the assessment.

4. EVALUATION PHASES

Three "evaluation" phases (Assessment, Report, and Recommendation) follow the "preliminary" phases.

4.1 ASSESSMENT PHASE

The assessment of the security product will be conducted in accordance with the security profile corresponding to the product (see section 2.3). The Assessment phase (figure 8) consists of three alternative tracks: (5a) Testing in-house at Navy facilities, (5b) Observing product performance at other activities, and (5c) Supporting product evaluation at other evaluation activities.

This document was originally developed to cover the (figure 8, 5a) Testing in-house track, where either (1) the vendor supplies the product to be tested, or (2) the Navy provides funding to acquire the product for testing. However, an alternative assessment track, first discussed in section 3.3.4, may be used to provide a less stringent evaluation of a product through (figure 8, 5b) observing the product in operation at a non-SPAWAR facility. A third possible track (5c in figure 8) is to support testing of the product at some evaluation facility (such as NSA or DISA), but that is outside the scope of this process.

The in-house testing track provides comprehensive testing in an SSC San Diego-controlled environment with on-site appraisal, and is the preferred track. The observing and supporting tracks offer quick-turnaround alternatives requiring minimal Navy resources.

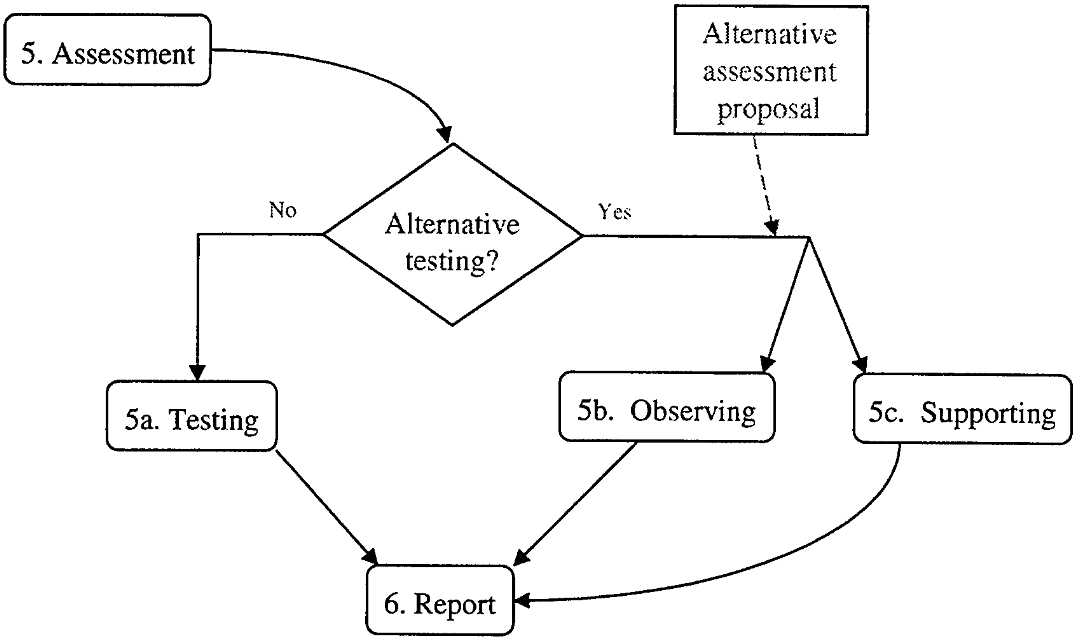


Figure 8. Assessment overview.

4.1.1 Testing Track

Figure 9 shows the most important segment of the entire evaluation process, where the product will be tested in a Navy laboratory environment that is similar to U.S. Navy operational environments. One or more of the SSC San Diego Information Assurance & Engineering Division (D87), Naval Research Laboratory (NRL), SSC Charleston, and support contractor INFOSEC laboratories provide such an environment.

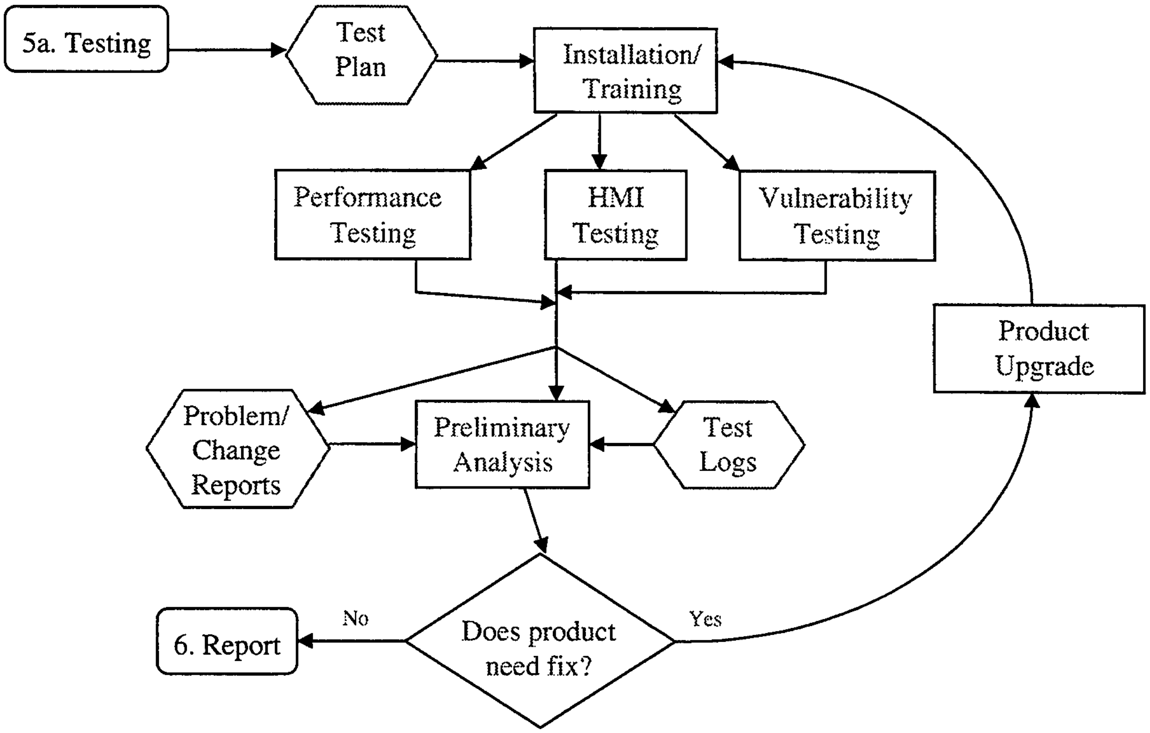


Figure 9. Testing track.

4.1.1.1 Test Plan. The first goal for this track is to develop a test plan (including test procedures) that is agreeable to both the Government and the vendor. This is generally initiated during the negotiation phase.

The test plan will discuss each requirement as established in the product category security profile. The test plan must establish major objectives that break down into testable objectives, with the passing criteria for each objective clearly stated. See section 5.3 for further details.

The test plan will be developed in accordance with the D87 documentation procedures and will undergo peer review as required.

4.1.1.2 Installation. The vendor is generally expected to make technical personnel available during the initial installation to ensure a proper configuration. Figure 10 shows a generic test configuration for testing security products in D87's Network Systems Security (NSS) Laboratory. Other equipment will be added to this basic configuration when needed on a case-by-case basis.

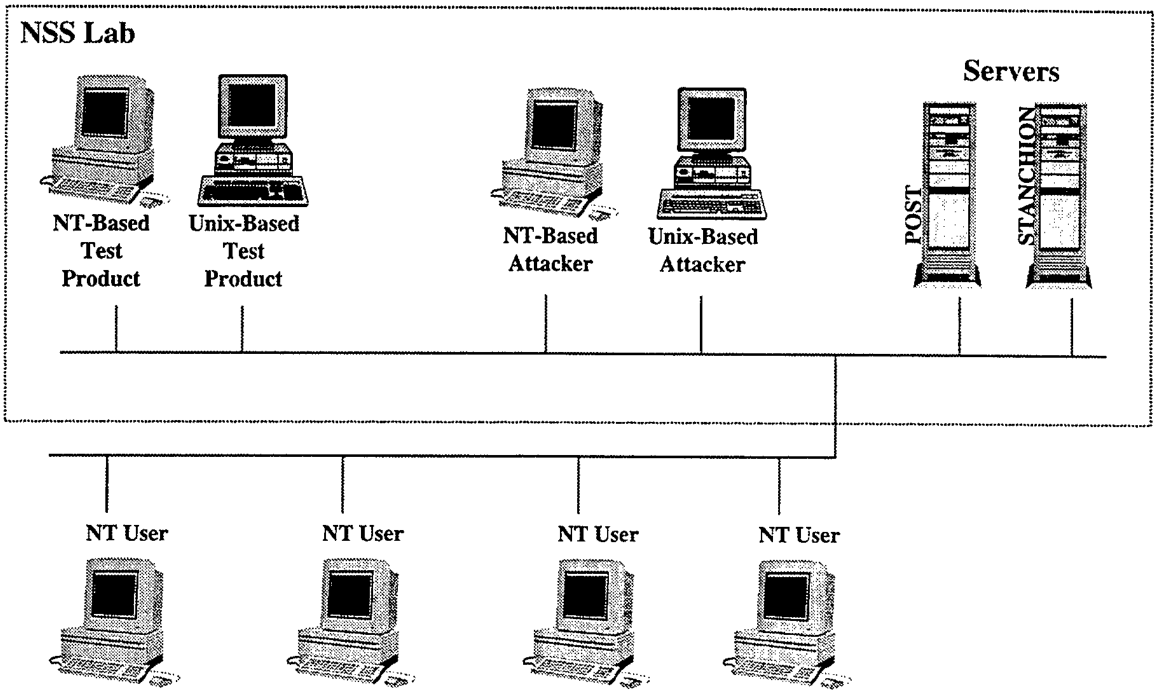


Figure 10. Generic test configuration.

4.1.1.3 Training. The vendor is expected to provide product training and/or training materials to the Government test team.

4.1.1.4 Product Testing. The three major areas of testing are performance, human–machine interface (HMI), and vulnerability. The development of specific security testing tools will be discussed in a separate security toolkit document.

4.1.1.4.1 Performance Testing. Performance testing assesses the product's functionalities to ensure the product performs as advertised and meets the requirements of the U.S. Navy. Each product category's security profile is associated with one or more protection profiles from the Common Criteria and security requirements. The development of performance criteria will be documented in a separate security profile document.

4.1.1.4.2 HMI Testing. HMI testing measures product usability for personnel of the U. S. Navy. HMI testing will ensure that the product's HMI design meets the needs of the U.S. Navy. Each product category's security profile is associated with a list of usability criteria derived from the Defense Information Infrastructure Common Operating Environment (DII COE) and security requirements. The development of HMI criteria will be documented in a separate security profile document.

4.1.1.4.3 Vulnerability Testing. The vulnerability testing determines security deficiencies of the product and measures the security performance of the product. Security deficiencies identify weaknesses through which the product may be attacked. Security performance is a measure of how well the product implemented security measures. The vulnerability testing will ensure that the product's security architecture meets the security requirements of the U.S. Navy. Each product category's security profile is associated with a list of vulnerability criteria derived from analyses of the vulnerabilities, threats, and countermeasures tied in to the security policies and security requirements based on the SECONOPS. The development of vulnerability criteria will be documented in a separate security profile document.

4.1.1.5 Analysis. The testers will analyze the test results in accordance with the test plan and the product specific test criteria specified in the security profile.

4.1.1.6 Possible Fixes. It is likely that the testing and analysis will uncover problems with the product and generate Problem/Change Reports (PCR). The vendor may be given the chance to make fixes or patches and submit the product for re-test under the same test procedures. The regression testing may be partial or full, depending on the scale of the change.

4.1.2 Observing Track

The observing track (figure 11), the alternative to in-house testing, may be used to provide a less stringent evaluation of a product through observing product performance at a non-SPAWAR facility.

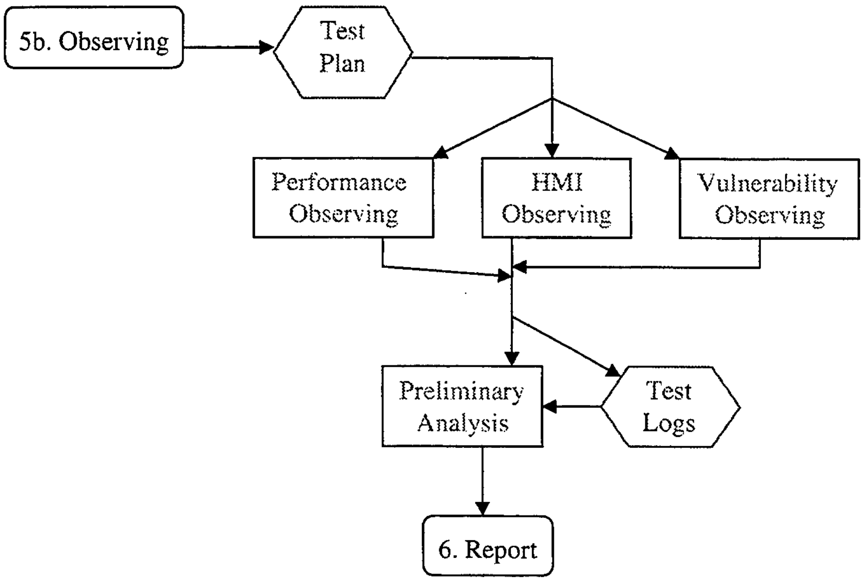


Figure 11. Observing track.

4.1.2.1 Test Plan. The first goal is to develop a test plan that establishes major objectives that are broken down into testable objectives, with the passing criteria for each objective clearly stated. The test plan will be developed in accordance with the D87 documentation procedures and will undergo peer review as required.

4.1.2.2 Training. The Government must acquire the product training materials and train the observing team.

4.1.2.3 Product Observing. The three major areas of interest are performance, HMI, and vulnerability.

4.1.2.3.1 Performance Observing. Performance observing assesses the product's functionalities to ensure that the product performs as advertised and meets requirements of the U.S. Navy. Each product category's security profile is associated with one or more protection profiles from the Common Criteria and security requirements. The development of performance criteria will be documented in a separate security profile document.

4.1.2.4.2 HMI Observing. HMI observing measures product usability for personnel of the U.S. Navy. HMI observing will ensure that the product's HMI design meets the needs of the U.S. Navy. Each product category's security profile is associated with a list of usability criteria derived from the DII COE and security requirements. The development of HMI criteria will be documented in a separate security profile document.

4.1.2.3.3 Vulnerability Observing. Vulnerability observing ensures that the product's security architecture meets the security requirements of the U.S. Navy. Each product category's security profile is associated with a list of vulnerability criteria derived from analyses of the vulnerabilities, threats, and countermeasures tied in to the security policies and security requirements based on the SECONOPS. The development of vulnerability criteria will be documented in a separate security profile document.

4.1.2.4 Analysis. Analysis of results will follow the criteria set forth in section 4.1.1.5. The analysis will, of course, be less rigorous as compared to the analysis from testing in-house.

4.1.3 Supporting Track.

The supporting track (figure 12), another alternative to in-house testing, may be used to provide a product evaluation that is less specific to U.S. Navy requirements through supporting product testing by a non-SPAWAR activity. SSC San Diego may participate as a test site, as exemplified by participation in the Security Proof of Concept Keystone (SPOCK) tests (see Appendix C for overview of the SPOCK process).

4.1.3.1 Test Plan. The first goal is still to develop a test plan that establishes major objectives that are broken down into testable objectives, with the passing criteria for each objective clearly stated. The test plan will be developed in accordance with the D87 documentation procedures and will undergo peer review as required.

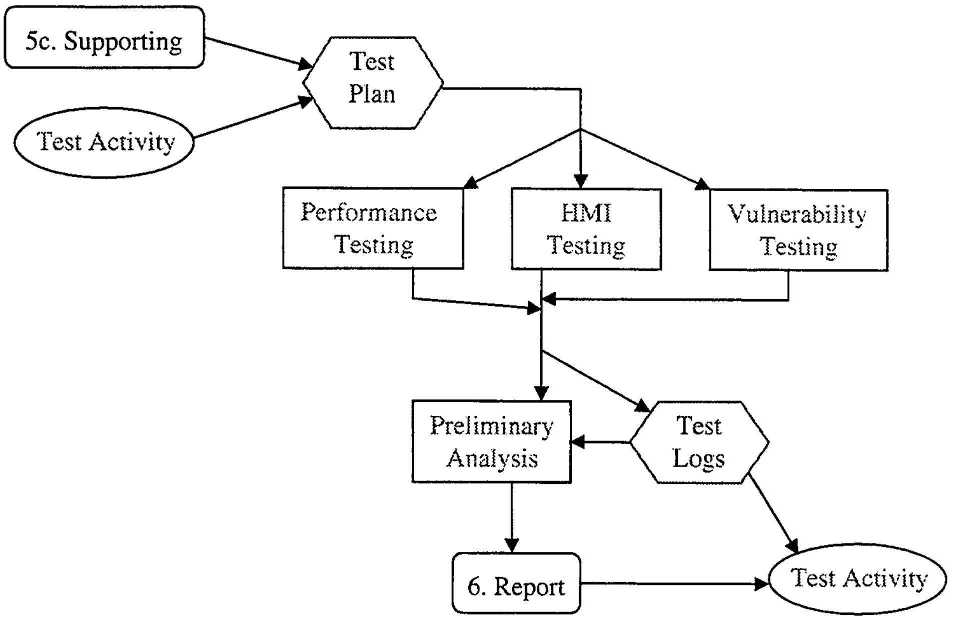


Figure 12. Supporting Track.

4.1.3.2 Training. The Government must acquire the product training materials and train the observing team.

4.1.3.3 Product Test Supporting. The three major areas of interest are performance, HMI, and vulnerability.

4.1.3.3.1 *Performance Testing.* Performance testing assesses the product's functionalities to ensure that the product perform as advertised and meets the requirements of the U.S. Navy. Each product category's security profile is associated with one or more protection profiles from the Common Criteria and security requirements. The development of performance criteria will be documented in a separate security profile document.

4.1.3.4.2 HMI Testing. HMI testing measures product usability for personnel of the U.S. Navy. HMI testing will ensure that the product's HMI design meets the needs of the U.S. Navy. Each product category's security profile is associated with a list of usability criteria derived from the DII COE and security requirements. The development of HMI criteria will be documented in a separate security profile documents.

4.1.3.3.3 Vulnerability Testing. The vulnerability testing ensures that the product's security architecture meets the security requirements of the U.S. Navy. Each product category's security profile is associated with a list of vulnerability criteria derived from analyses of the vulnerabilities, threats, and countermeasures tied in to the security policies and security requirements based on the SECONOPS. The development of vulnerability criteria will be documented in a separate security profile document.

4.1.3.4 Analysis. Analysis of results will follow the criteria set forth in section 4.1.1.5. The analysis may be less rigorous as compared to the analysis from testing in-house, and will likely be incorporated into the test report of the evaluation activity.

4.2 REPORT PHASE

The test and analysis results are compiled into an evaluation report, mapping the test results to the applicable functional and security requirements of the applicable product category. The report will then undergo the D87 formal inspection process. The sponsor may be offered the opportunity to provide technical input through observing the formal inspection. Figure 13 shows the report development process.

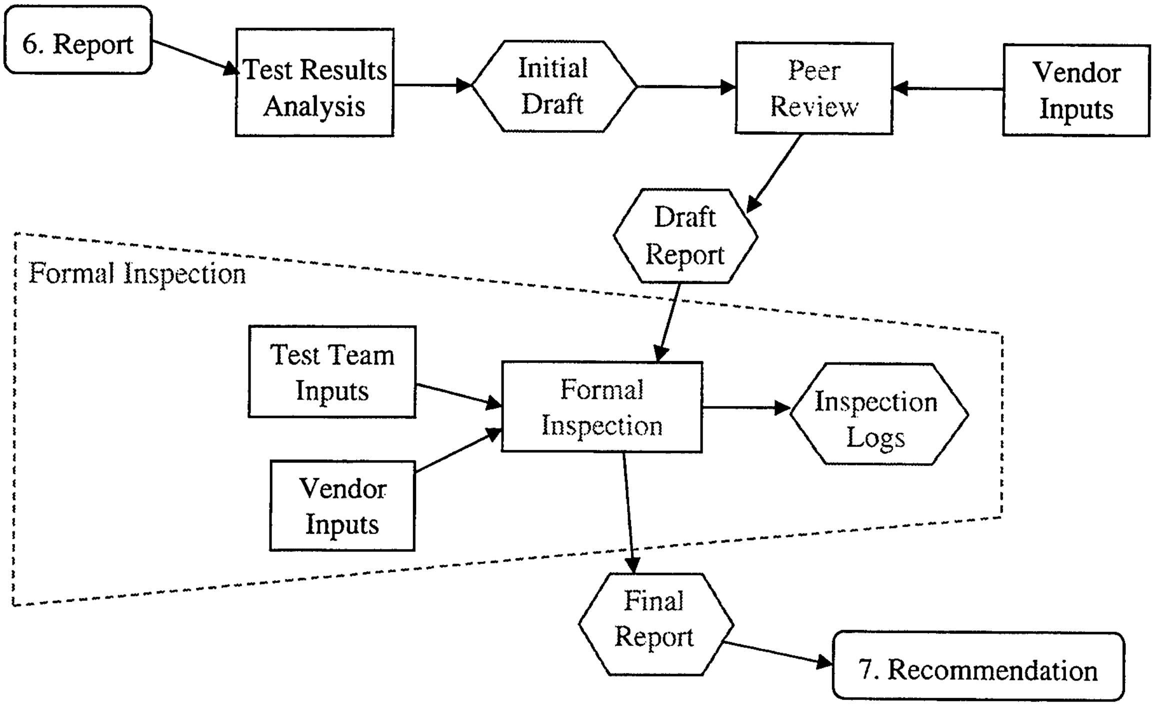


Figure 13. Report phase.

4.2.1 Draft Report

After the report is first compiled into an "initial draft," it will be distributed to the testers, vendor representative, and other technically proficient personnel for a peer review. The revised report resulting from the peer review will be submitted to the D87 formal inspection process as the "draft report."

4.2.2 Formal Inspection

Figure 14 is an overview of the D87 formal inspection process, which is further detailed in Appendix B. The boxed area of figure 14 is an expansion of the boxed area in figure 13.

Some advantages of the formal inspection process are:

- Defined limit on the review period.
- Inspectors from different disciplines, including persons unfamiliar with the subject, provide diverse views.
- Standardized defect rules.
- Inspection meeting that resolves all the submitted defects.

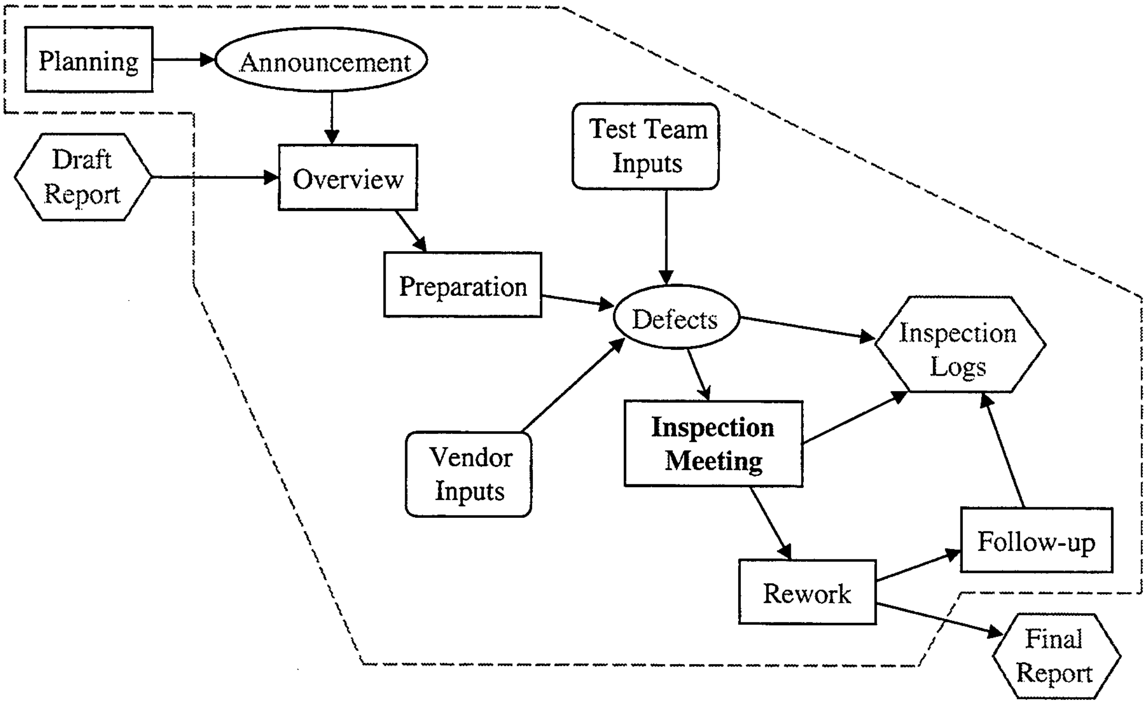


Figure 14. Formal inspection process.

4.2.3 Final Report

All discrepancies identified during the formal inspection will be resolved and a final report delivered to the sponsor.

4.3 RECOMMENDATION PHASE

The evaluation report will include a recommendation to the sponsor regarding what to do next about the product: use, reject, or test more. This phase (see figure 15) is deliberately separated from the report phase to emphasize the recommended options.

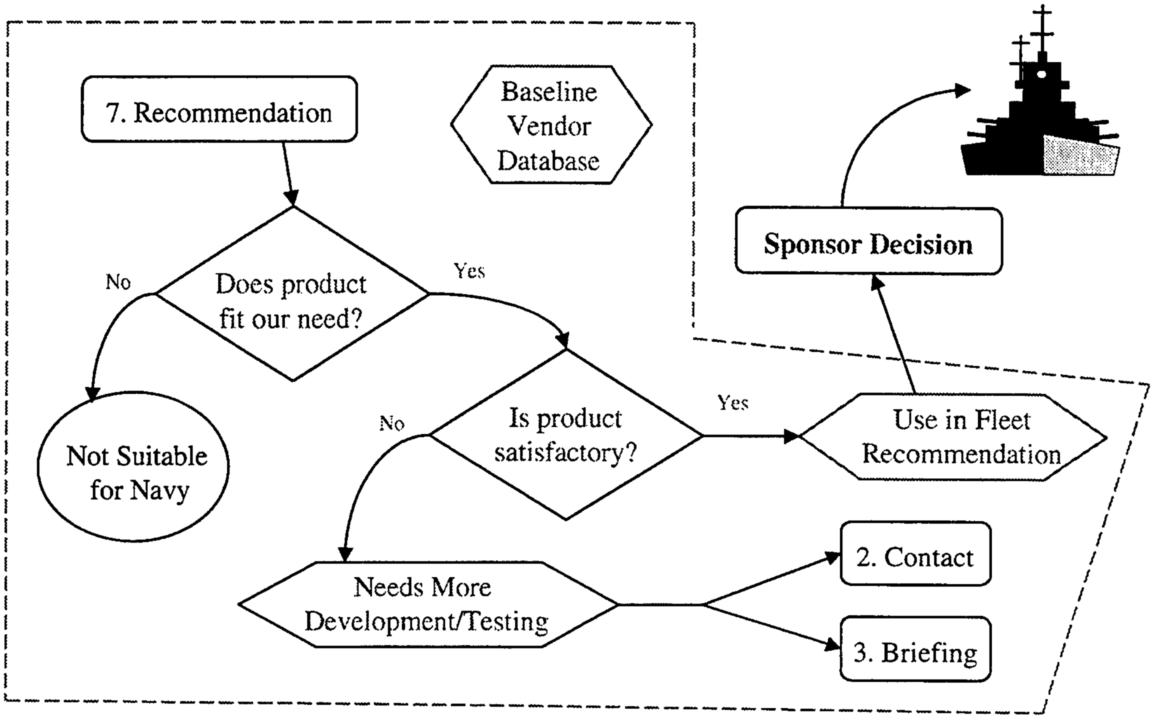


Figure 15. Recommendation phase.

4.3.1 Rejection

If the product is determined as unsuitable for the Navy, then the process terminates.

4.3.2 Use

If the product is suitable for the Navy, then answer the question of whether the product is ready for use. If yes, then recommend use of the product in fleet systems, and the process terminates.

4.3.3 Additional Evaluation

If the product is not quite ready for use because of lack of maturity or some technical problem, then recommend additional assessment. The evaluation process then restarts, either in contact or briefing phases.

5. DOCUMENTATION

5.1 VENDOR DATABASE

A database should be generated for each vendor/product evaluated. The database will include all the information collected through all phases of the process.

5.2 PRELIMINARY RESULTS

The following items are some of the information that should be included in the database:

- Research decision regarding whether the vendor/product fits a need of the U.S. Navy.
- Contact results from discussions with vendor.
- Questionnaire results from vendor and other sources.
- Presentation made by the vendor.
- Briefing and meeting minutes.
- Assessment agreement negotiated by the Government and the vendor.
- Security profile that the product will be evaluated against.

5.3 TEST PLAN

The test plan must establish the major objectives of the assessment. Each major objective shall be broken down into testable objectives, with the passing criteria for each objective clearly stated.

The test plan will be developed in accordance with D87 documentation procedures and will undergo peer review as required. The objectives and passing criteria in the test plan shall be based on the security profile as defined in section 2.3.1.

5.4 TEST LOGS/PCRS

The logs from the assessment are retained for historical background. The test logs include all information recorded during the assessment, all submitted Problem/Change Reports (PCR), meeting minutes, test results, and test configuration changes, etc.

5.5 EVALUATION REPORT

5.5.1 Initial Draft

The initial draft of the evaluation report outlines the history and results of the evaluation. This is distributed to the test team, the vendor technical support personnel, if applicable, and technical experts for review and to elicit comments (peer review).

5.5.2 Draft Report

The draft report constitutes the starting point of the formal inspection process and integrates comments and contributions from the peer review.

5.5.3 Final Report

The final report results from the formal inspection and is the evaluation product delivered to the sponsor.

5.5.4 Formal Inspection Logs

The logs from the formal inspection are retained for historical background, including the number of submitted defects and the amount of work performed during the formal inspection process.

6. GLOSSARY

Table 4. Acronyms and terminology.

Acronym	Meaning
CC	Common Criteria
CCEB	Common Criteria Editorial Board
CM	Configuration Management
CMM	Capability Maturity Model. A software engineering process improvement model (SEI CMM) or a security engineering process improvement model (NSA's SSE CMM)
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria (Canadian standard)
DIAP	Defense Information Assurance Program (DoD program)
DII COE	Defense Information Infrastructure Common Operating Environment
DISA	Defense Information Systems Agency
DoD	Department of Defense
EAL	CC Evaluated Assurance Levels
FI	Formal Inspection
FIPS	Federal Information Processing Standards (NIST)
Firewall	Application that provides controlled and audited access to services, both from inside and outside of the network, by allowing, denying, and/or redirecting the flow of data
GOTS	Government off-the-shelf
HAG	High assurance guards
HMI	Human–machine interface (usability or ease-of-use)
IDS	Intruder Detection Systems
INFOSEC	Information Systems Security
ISO	International Organization for Standardization
IT21	Information Technology for 21st Century
Iterative	Repetitive process in which each cycle of phases build on the previous cycle
ITSC	Information Technology Service Center
ITSEC	Information Technology System Evaluation Criteria (European standard)

Table 4. Acronyms and terminology. (continued)

Acronym	Meaning
LAN	Local Area Network
LCMA	Life Cycle Management Agent
LCS	Life Cycle Support
MLS	Multi-Level Security
NDI	Non-Developmental Item
NIAP	National Information Assurance Partnership (NSA program)
NIST	National Institute of Standards and Technology, a Department of Commerce agency
N/MCI	Navy/Marine Corps Intranet, formerly Naval Intranet (NI), Navy Wide Intranet (NWI), and Navy Virtual Intranet (NVI)
NRL	Naval Research Laboratory
NSA	National Security Agency
NSS	Network Systems Security
Orange Book	DoD security standard “DoD 5200.28-STD”
PCR	Problem/Change Report
Performance	Measure of how well a product performs its functions
PP	CC Protection Profile
Rapid prototyping	Systems engineering process that develops of a first, quick version of a product; provides immediate feedback to the user
Scalability	Measure of how a product can be used by organizations of different sizes
SECONOPS	Security Concept of Operations
SEI	Software Engineering Institute
SP	Security profile; D87-defined overall profile for a product category that includes protection profile(s)
SPAWAR	Space and Naval Warfare Systems Command
SSC San Diego	Space and Naval Warfare Systems Center San Diego
Spiral model	Iterative systems engineering process with four quadrants (planning, risk analysis, engineering, and customer evaluation)
SPOCK	Security Proof of Concept Keystone (NSA program)
SSE	Systems Security Engineering
ST	CC Security Target
TCSEC	Trusted Computer System Evaluation Criteria (USA standard)

Table 4. Acronyms and terminology. (continued)

Acronym	Meaning
Test Plan	Plan detailing how the evaluation is to be performed
TPEP	Trusted Product Evaluation Program (NSA program)
VPN	Virtual Private Network
Vulnerability	Security weaknesses present in the product

APPENDIX A

COMMON CRITERIA PROTECTION PROFILE

A.1 INTRODUCTION

In 1990, the International Organization for Standardization (ISO) began to develop an international standard evaluation criteria for general use. The purpose of the new criteria was to fulfill the need for mutual recognition of standardized security evaluation results in the global Information Technology (IT) market. These criteria were named the "Common Criteria for Information Technology Security Evaluation" and sponsored by the following organizations:

- Canada's Communications Security Establishment,
- France's Service Central de la Sécurité des Systèmes d'Information,
- Germany's Information Security Agency,
- The Netherlands National Communications Security Agency,
- The United Kingdom's Communications Electronics Security Group,
- The United States' National Security Agency (NSA) and National Institute of Standards and Technology (NIST).

A.2. BACKGROUND

In June 1993, these sponsoring organizations pooled their efforts and began a joint activity to align their separate criteria into a single set of IT security criteria that could be used worldwide. This activity was named the Common Criteria (CC) Project and its purpose was to resolve the conceptual and technical differences found in the source criteria and to deliver the results to ISO as a contribution to the international standard under development. Representatives of the sponsoring organizations formed the Common Criteria Editorial Board (CCEB) to develop common criteria for information technology security evaluations.

A.2.1 Revisions

Common Criteria for Information Technology Security Evaluation, Version 1.0, was completed by the CCEB in January 1996 and approved by ISO in April 1996 for distribution as a Committee Draft.

Common Criteria for Information Technology Security Evaluation, Version 2.0, was officially adopted by the sponsoring nations in October 1998.

A.2.2 Assurance Requirements

Table A-1 maps the CC Evaluated Assurance Levels (EAL) to the assurance classes/ families/components.

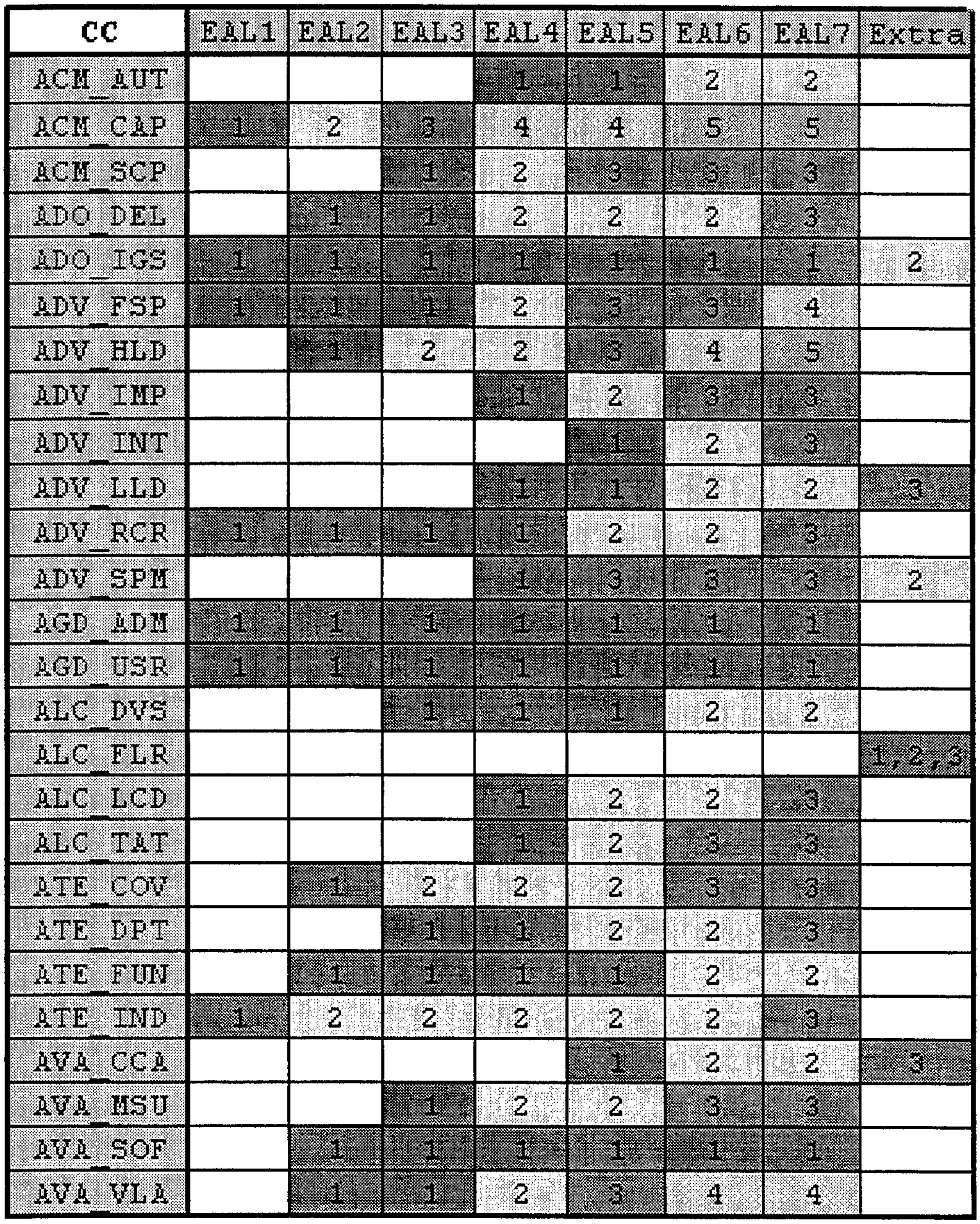
A.2.2.1 Assurance Class/Family/Component. There are seven (7) classes of assurance families in Common Criteria: Configuration Management (CM), Delivery Operations, Development, Guiding Documents, Life Cycle Support (LCS), Tests, and Vulnerability Assessment. Each assurance class has several assurance families associated with it. For example, the CM class has three families: ACM_AUT (automation), ACM_CAP (capabilities), and ACM_SCP (scope). Each assurance family may have several components, such as ACM_CAP.1, ACM_CAP.2, and ACM_CAP.3, where the assurance generally increases with the component number. The components are the numbers shown in table A-1.

A.2.2.2 EAL Requirements

Each EAL requires certain level of assurance in various assurance families shown in its corresponding column in Table A-1. For example, a system is rated as EAL2 if it satisfies the requirements for **ACM_CAP.2**, ADO_DEL.1, ADO_IGS.1, ADV_FSP.1, ADV_HLD.1, ADV_RCR.1, AGD_ADM.1, AGD_USR.1, ATE_COV.1, ATE_FUN.1, **ATE_IND.2**, AVA_SOF.1, and AVA_VLA.1.

A system can be rated as EALx+ if it satisfies all the requirements for EALx plus some other requirement(s), but not enough to reach the next EAL. For example, a system is rated as EAL1+ if it satisfies the requirements for ACM_CAP.1, ADO_IGS.1, ADV_FSP.1, ADV_RCR.1, AGD_ADM.1, AGD_USR.1, and ATE_IND.1, **plus ADV_HLD.2 and ATE_COV.1**.

Table A-1. Common Criteria overview.



	CC	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	Extra
CM	ACM_AUT				1	1	2	2	
	ACM_CAP	1	2	3	4	4	5	5	
	ACM_SCP			1	2	3	3	3	
Operations Delivery	ADO_DEL		1	1	2	2	2	3	
	ADO_IGS	1	1	1	1	1	1	1	2
Development	ADV_FSP	1	1	1	2	3	3	4	
	ADV_HLD		1	2	2	3	4	5	
	ADV_IMP				1	2	3	3	
	ADV_INT					1	2	3	
	ADV_LLD				1	1	2	2	3
	ADV_RCR	1	1	1	1	2	2	3	
	ADV_SPM				1	3	3	3	2
Document Guidanc	AGD_ADM	1	1	1	1	1	1	1	
	AGD_USR	1	1	1	1	1	1	1	
LC	ALC_DVS			1	1	1	2	2	
	ALC_FLR								1,2,3
	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	
Test	ATE_COV		1	2	2	2	3	3	
	ATE_DPT			1	1	2	2	3	
	ATE_FUN		1	1	1	1	2	2	
	ATE_IND	1	2	2	2	2	2	3	
Assessmen Vulnerability	AVA_CCA					1	2	2	3
	AVA_MSU			1	2	2	3	3	
	AVA_SOF		1	1	1	1	1	1	
	AVA_VLA		1	1	2	3	4	4	

A.2.3 Evaluation Comparison

CC-based evaluation results can be compared to evaluation results from previous standards of the sponsoring organizations:

- USA's Trusted Computer System Evaluation Criteria (TCSEC) and Trusted Product Evaluation Program (TPEP)
- Europe's Information Technology System Evaluation Criteria (ITSEC)
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

Table A-2 summarizes the relationship between the various security evaluation standards. For example, a TPEP B2 class system is equal to a CC EAL5 system, or an ITSEC rating E4, or CTCPEC rating of T4.

Table A-2. Common Criteria comparisons.

Common Criteria (World)	ITSEC (Europe)	CTCPEC (Canada)	TCSEC/TPEP (USA)	Assurance Level	Maximum Risk Index	Security Op Mode
		T7		Very High	4	ML
EAL7	E6	T6	A1			
EAL6	E5	T5	B3	High	3	
EAL5	E4	T4	B2		2	Partitioned ML
		T3		Medium	1	Partitioned
EAL4	E3	T2	B1	Low		
EAL3	E2	T1	C2		0	System High
EAL2	E1		C1			Dedicated
EAL1				None	0	
EAL0	E0	T0	D			

A.2.3.1 Assurance Level. The assurance level is a descriptive rating of how closely each system follows the specified security requirements.

A.2.3.2 Maximum Risk Index. The maximum allowed risk index is defined as:

$$\text{Maximum Risk Index} = \begin{cases} R_{max} - R_{min} & R_{max} >= R_{min} \\ 0 & R_{max} < R_{min}, \end{cases}$$

where R_{max} is the maximum data sensitivity (see table A-3) and R_{min} is the minimum user clearance (see table A-4).

Table A-3. Maximum data sensitivity.

Maximum Data Sensitivity Ratings[1] Without Categories	RATING (R_{max})	Maximum Data Sensitivity With Categories[2]	RATING (R_{max})
Unclassified	0	Not Applicable[3]	
Not Classified but Sensitive[4]	1	N With One or More Categories	2
Confidential	2	C With One or More Categories	3
Secret	3	S With One or More Categories With No More Than One Category Containing Secret Data S With Two or More Categories Containing Secret Data	4 5
Top Secret	5	TS With One or More Categories With No More Than One Category Containing Secret or Top Secret Data TS With Two or More Categories Containing Secret or TS Data	6 7

Table A-4. Maximum user clearance.

MINIMUM USER CLEARANCE	RATING (R_{min})
Uncleared (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)/Current Background Investigation (BI)	4
Top Secret (TS)/Current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

A.2.3.3 Security Mode of Operation. This is the mode of security operation required to satisfy each EAL. The security modes are Multi-Level (ML), Partitioned ML, Partitioned, System High, and Dedicated.

A.2.4 References

Until the advent of Common Criteria, the security standard was the "Orange Book":

- *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985. DoD 5200.28-STD.

The Common Criteria standards are:

- *Common Criteria for Information Technology Security Evaluation.* 31 January 1996. CEB-96/011. Version 1.0.
- *Common Criteria for Information Technology Security Evaluation.* May 1998. CCIB-98-026. Version 2.0.
- Common Criteria for Information Technology Security Evaluation. August 1999. CCIB-99-031. Version 2.1.

A.3 APPLICATION

The Common Criteria provide guidance to develop implementation-independent Protection Profiles (PP), and implementation-dependent security targets (ST).

A.3.1 Protection Profile

The PP defines security requirements for IT product categories such as operating systems, firewalls, intruder detection systems (IDS), mail guards, virtual private networks (VPN), and audit data reduction tools. PPs can also be developed for a system of products, such as the entire installation of IT products aboard a ship. PPs are intended to be reusable by all products or systems within that same category. A PP provides consumers with a means of referring to a specific set of security requirements and objectives, and facilitates evaluations against these objectives. The PP also provides the rationale for the security requirements and objectives.

A.3.2 Security Target

The ST defines security requirements for specific products such as UNIX and NT operating systems, high assurance guards (HAG), and multi-level security (MLS). These requirements may be defined by reference to a PP, directly by reference to Common Criteria functional or assurance components, or stated explicitly. The ST contains the IT product summary specification, together with the security requirements and objectives, and the rationale for each requirement. The ST is the basis for agreement between all parties as to what security features the IT product must provide.

A.3.3 COTS Product Evaluation

PPs are the basis for the D87 COTS network software security product evaluation process. PPs will provide the needed information to develop a product-screening questionnaire for selecting products for evaluation. Once specific products are selected for evaluation, the PP provides the basis to develop criteria against which the product will be evaluated. The PP will become part of the security profile, as defined by D87, developed for the product category. The product evaluation results will be mapped to the requirements shown in table A-1 and an Evaluated Assurance Level assigned for that product.

APPENDIX B

FORMAL INSPECTION PROCESS

B.1 INTRODUCTION

Formal Inspections (FI) have been used in the software industry since the 1970s. An FI eliminates defects in work products early and efficiently, thereby decreasing the development cost. Formal inspections thus improve overall software quality and reduce product cost.

The FI process is a defined, structured, and disciplined method for finding defects in any software work product at any stage of its development or maintenance. Past work products submitted to this process include operational concept documents, requirements specifications, development plans, design specifications and standards, program source code, test plans and procedures, and test reports.

B.2 SSC SAN DIEGO

More than a dozen projects at Space and Naval Warfare (SPAWAR) Systems Center, San Diego (SSC San Diego) have made the initial investment of training and implementation of FIs. These projects found and resolved defects in work products at an average cost of 1.5 staff hours per defect, or about $100. Conversely, finding and correcting a defect in a delivered/fielded work product is $1000 or more. Consequently, FIs produced significant cost savings.

In addition to higher quality work products and overall cost savings, benefits noted from the implementation of FIs at SSC San Diego included improvements in team synergy, staff morale, depth of technical knowledge, pride of authorship, development process, and project standards.

B.3 SSC SAN DIEGO D87

SSC San Diego D87 has implemented the formal inspection process as part of the drive toward compliance with the Software Engineering Institute's Capability Maturity Model (SEI CMM). All products released outside of D87 must now undergo formal inspection before release.

B.3.1 Formal Inspection Benefits

Some of the benefits of the formal inspection process include the following:

- Defined limit on the review period.
- Inspectors from different disciplines, including persons unfamiliar with the subject, to provide a diverse views.
- Standardized defect rules.
- Inspection meeting that resolves all the submitted defects.

B.3.2 Phase Diagrams

Figure B-1 is an overview of the six-phase formal inspection process as practiced by SSC San Diego D87. Figures B-2 through B-7 are more detailed breakdowns of the formal inspection phases and taken from the *Formal Inspection Process, Version 2.2*, dated 29 September 1997.

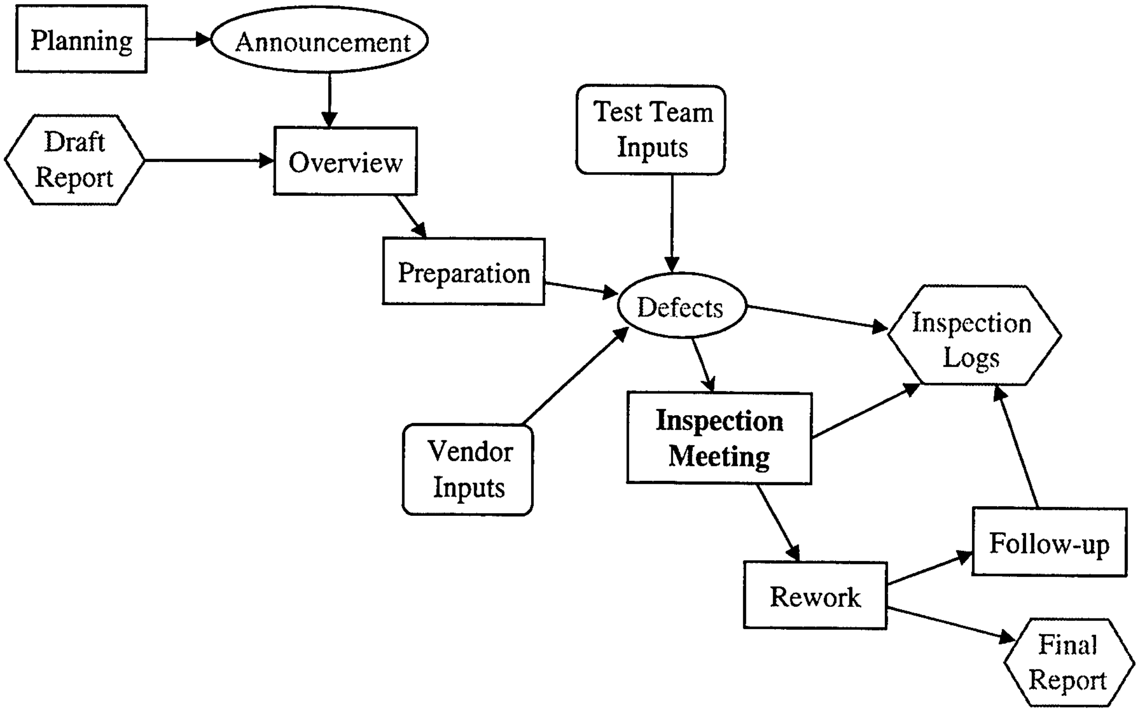


Figure B-1. Formal inspection overview.

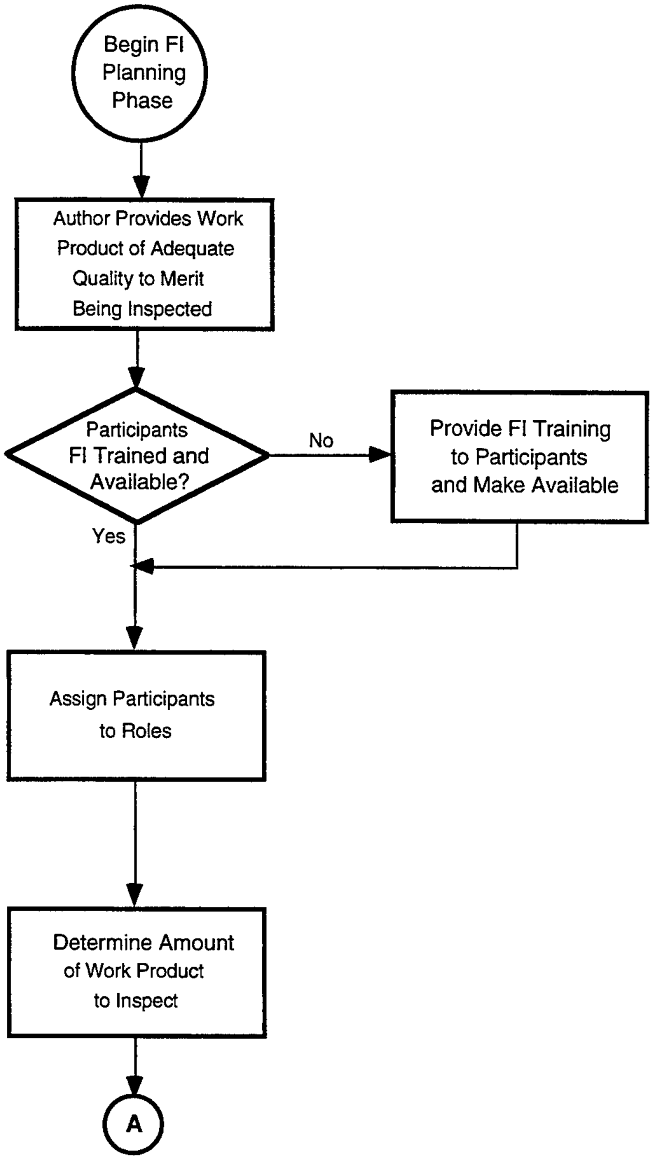

Begin FI Planning Phase
Author Provides Work Product of Adequate Quality to Merit Being Inspected
Participants FI Trained and Available?
No
Provide FI Training to Participants and Make Available
Yes
Assign Participants to Roles
Determine Amount of Work Product to Inspect
A

Figure B-2. Planning phase.

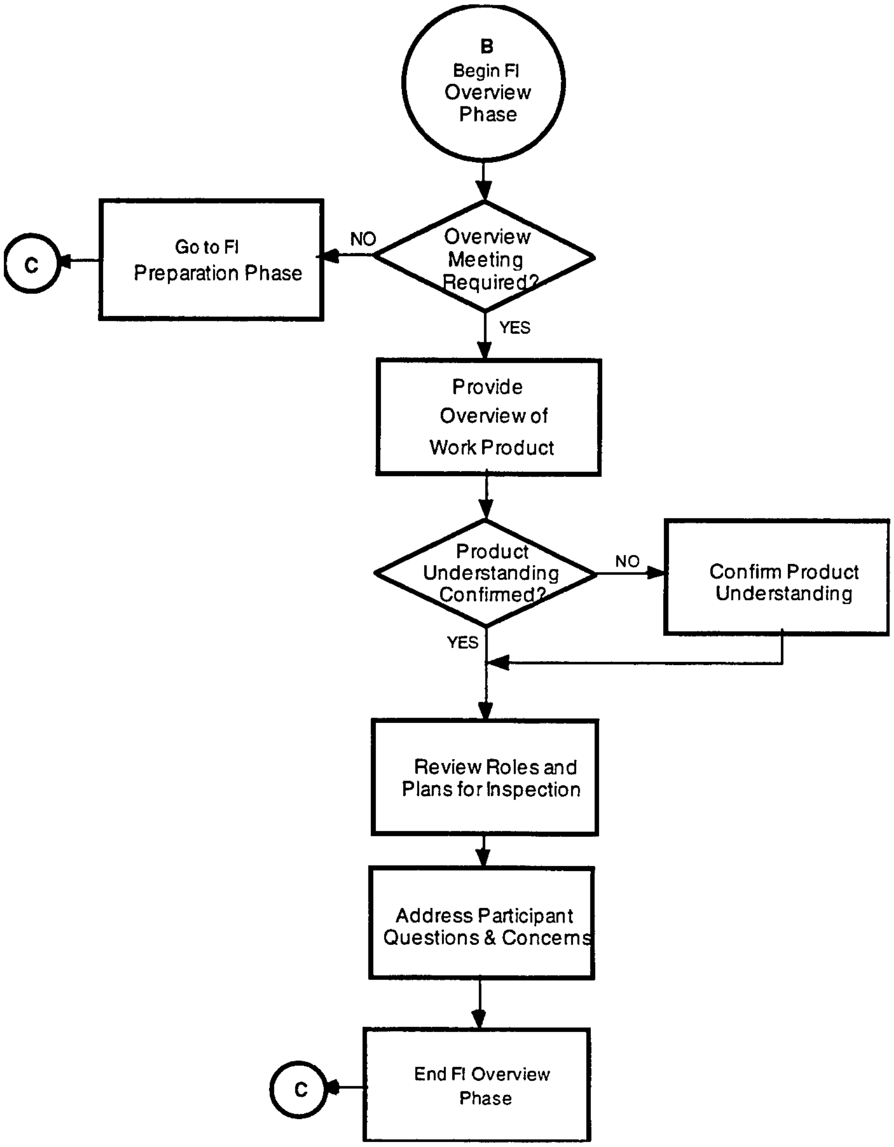


Figure B-3. Overview phase.

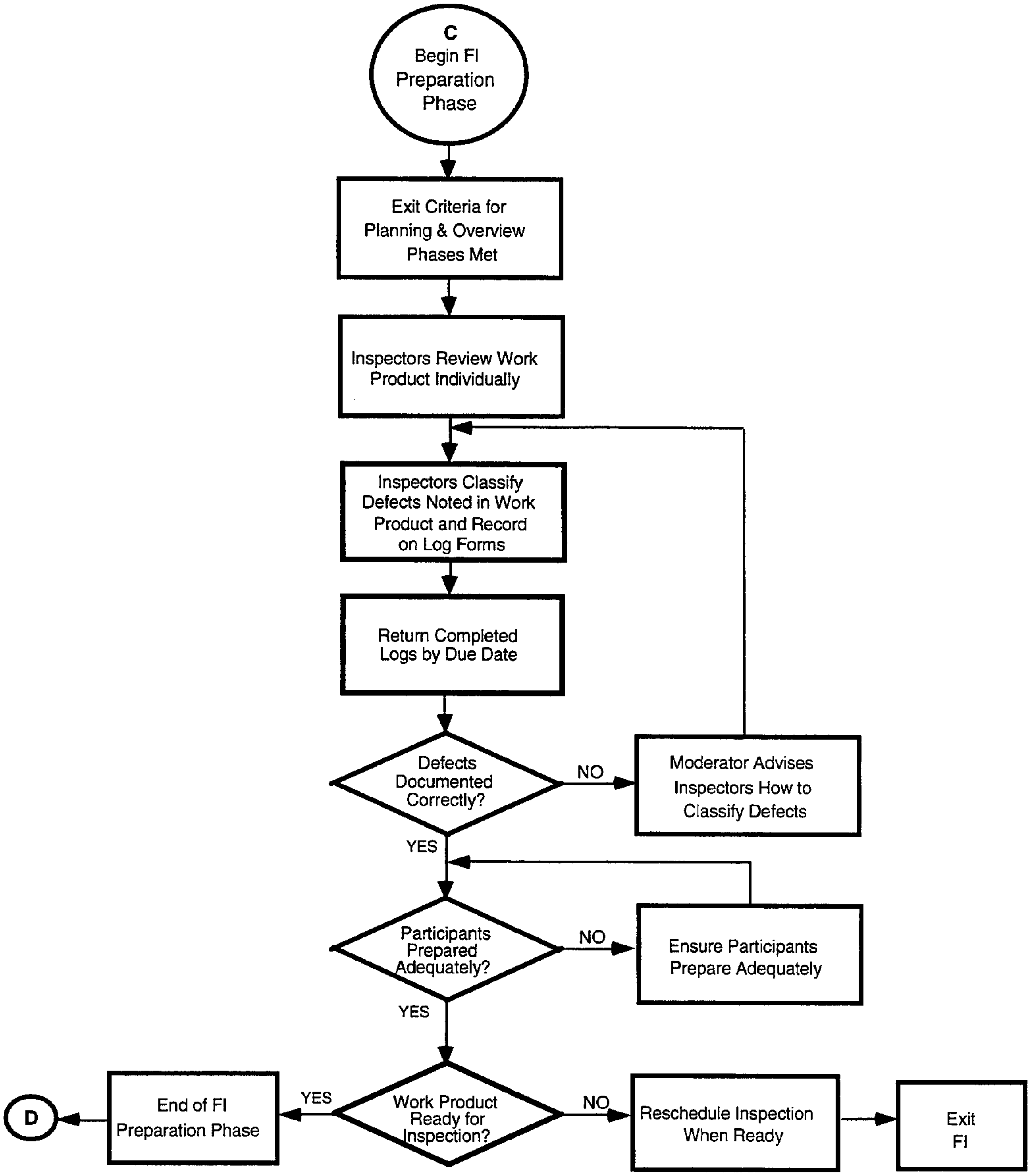

C
Begin FI Preparation Phase
Exit Criteria for Planning & Overview Phases Met
Inspectors Review Work Product Individually
Inspectors Classify Defects Noted in Work Product and Record on Log Forms
Return Completed Logs by Due Date
Defects Documented Correctly?
NO
Moderator Advises Inspectors How to Classify Defects
YES
Participants Prepared Adequately?
NO
Ensure Participants Prepare Adequately
YES
Work Product Ready for Inspection?
YES
End of FI Preparation Phase
D
NO
Reschedule Inspection When Ready
Exit FI

Figure B-4. Preparation phase.

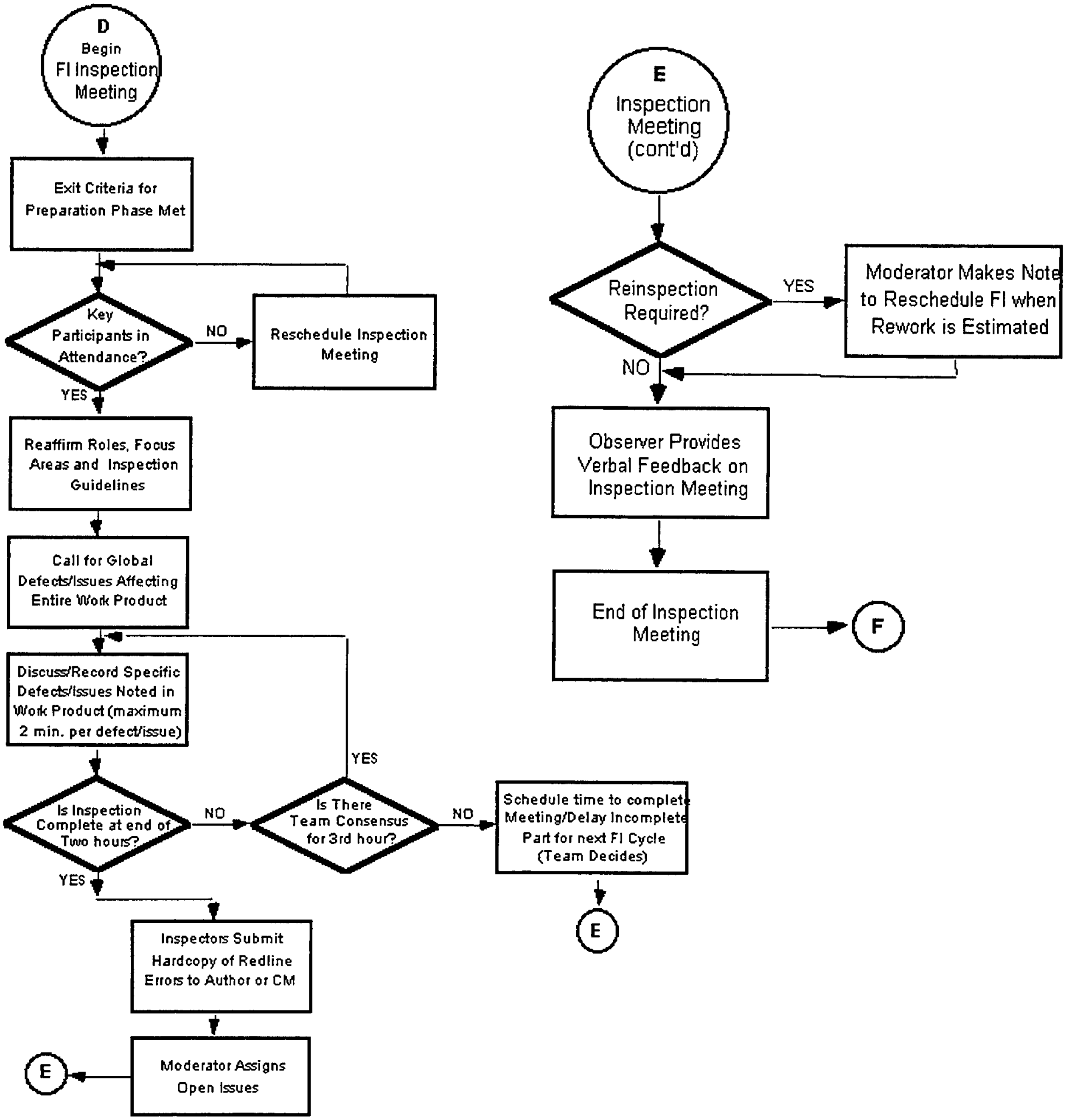


Figure B-5. Inspection meeting phase.

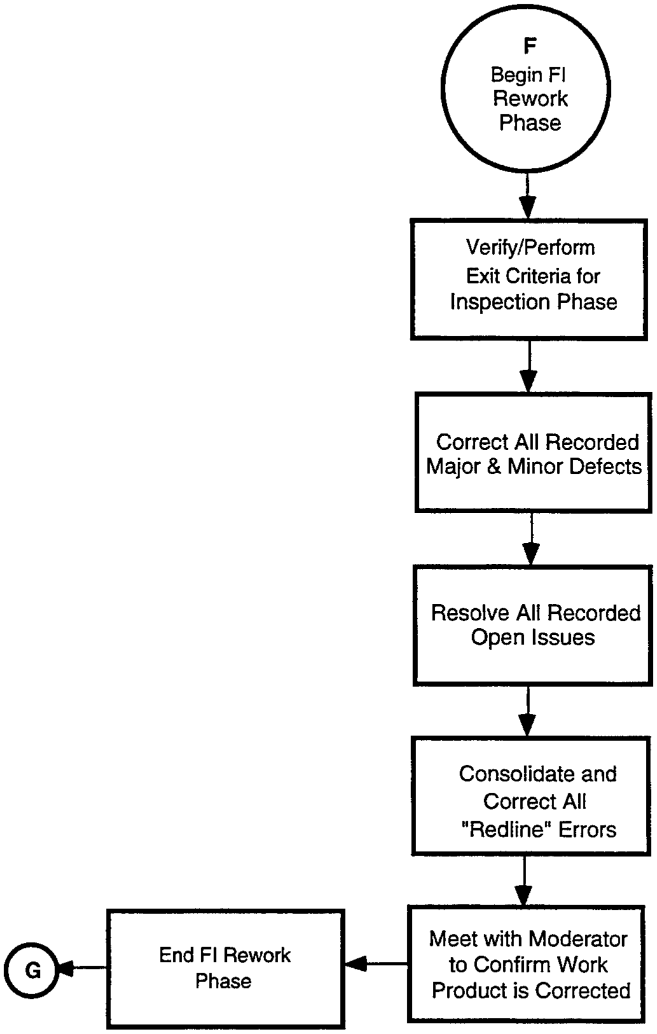


Figure B-6. Rework phase.

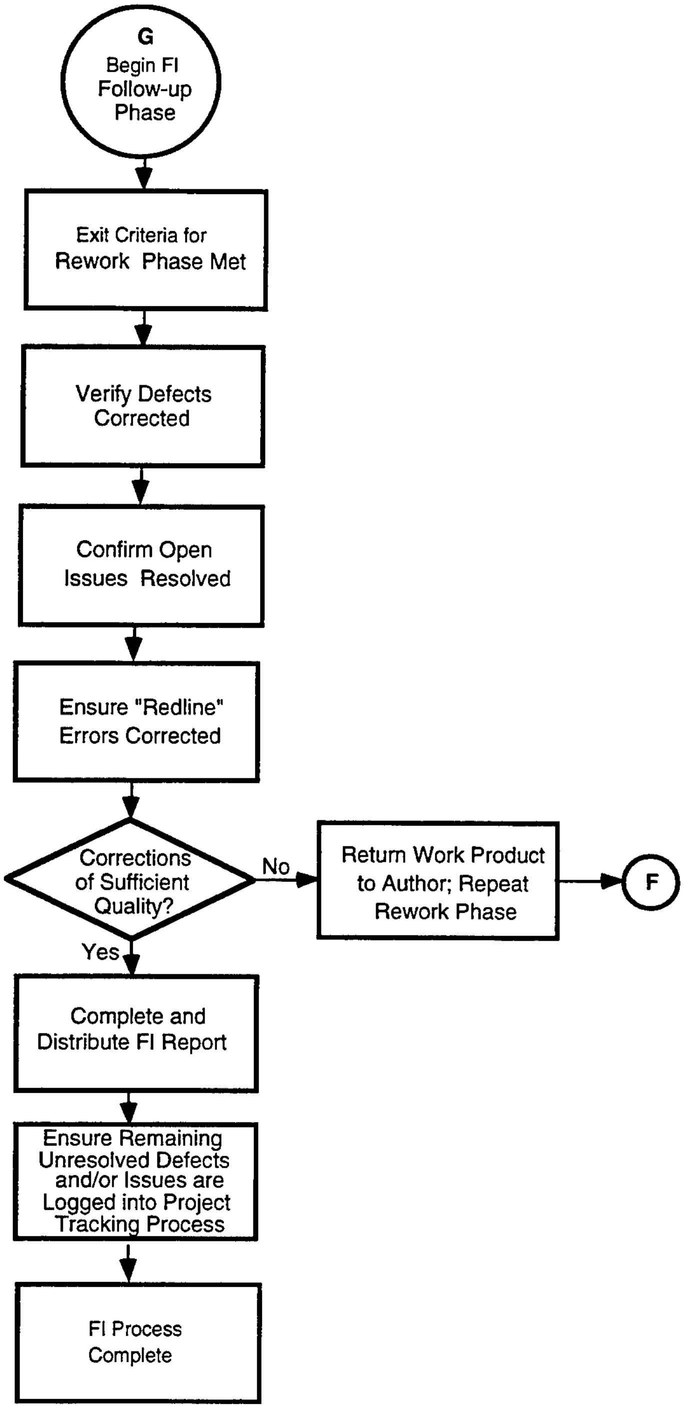

G
Begin FI Follow-up Phase
Exit Criteria for Rework Phase Met
Verify Defects Corrected
Confirm Open Issues Resolved
Ensure "Redline" Errors Corrected
Corrections of Sufficient Quality?
No
Return Work Product to Author; Repeat Rework Phase
F
Yes
Complete and Distribute FI Report
Ensure Remaining Unresolved Defects and/or Issues are Logged into Project Tracking Process
FI Process Complete

Figure B-7. Follow-up phase.

APPENDIX C

SPOCK EVALUATION PROCESS OVERVIEW

C.1 BACKGROUND

The Security Proof of Concept Keystone (SPOCK) program is a joint Government–Industry consortium sponsored by the National Security Agency (NSA) to demonstrate security features of commercial and Government products that can support dependable security architectures. SPOCK provides a forum for Government users and security technology providers to share information on security requirements, emerging technologies, and new product developments. Integrators and product developers are afforded opportunities to share new solutions, identify Government developed technology available for commercial use, and prototype commercial off-the-shelf (COTS) security products in Government-sponsored test beds.

C.2 SPOCK EVALUATION PROCESS

SSC San Diego D87 has participated as a test site in several SPOCK tests of COTS security products. SPOCK's evaluation process was analyzed and is shown in figure C-1.

- The starting point of this process is the regular vendor presentations, which could be initiated by SPOCK, the vendors, or sponsors (users, acquisition managers, evaluators, and program offices).
- If there is sufficient interest after the presentation, then SPOCK negotiates with the vendor regarding participation in a SPOCK evaluation.
- Upon agreement to test, then the vendor will generate claims and test scripts that verify these claims.
- After review and approval of the claims and scripts, then the vendor trains Government personnel to use the product.
- The testing will be conducted by Government personnel with vendor support.
- SPOCK will generate a product evaluation report based on the test reports submitted by the test sites.

C.3 SSC SAN DIEGO PARTICIPATION

SSC San Diego D87's participation in the SPOCK process can begin at various points in the SPOCK process:

- At the training phase (minimal involvement, just testing).
- At the script development/review phase.
- Initiates the SPOCK process for a product (effectively acting as a sponsor).

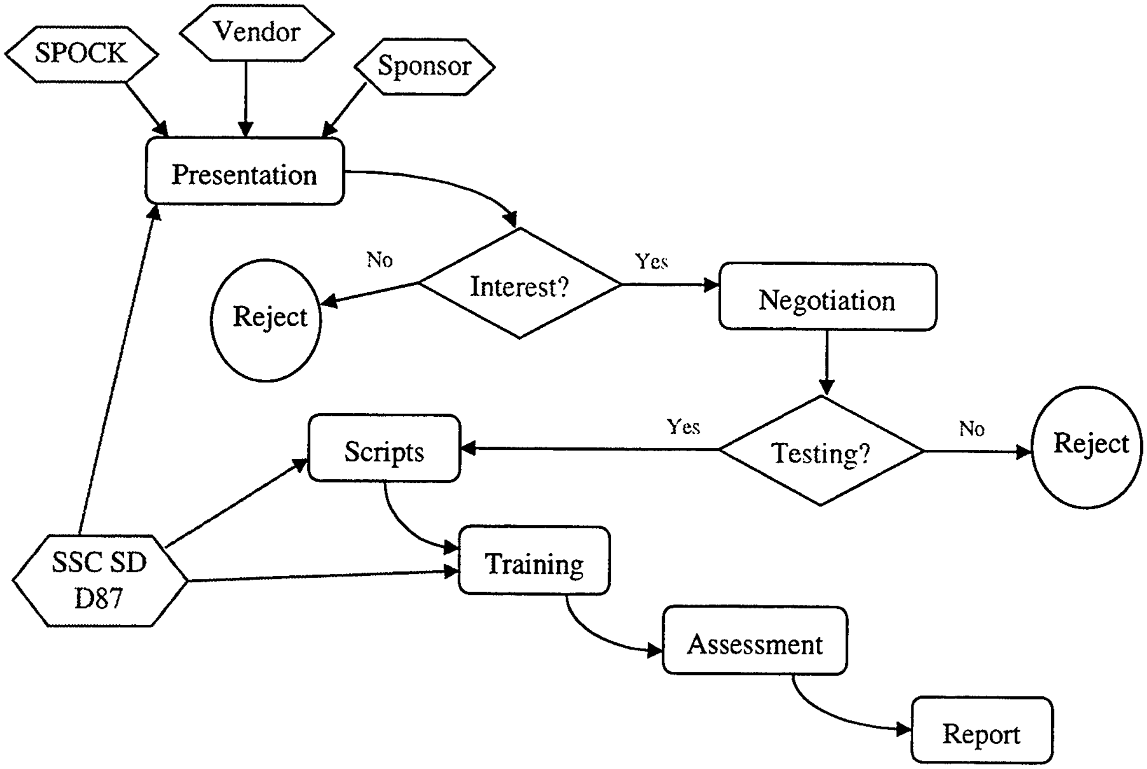


Figure C-1. SPOCK evaluation process.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
January 2000

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
COMMERCIAL OFF-THE-SHELF (COTS) SECURITY PRODUCTS EVALUATION PROCESS

5. FUNDING NUMBERS
PE: 0303140N
AN: DN3-5459
WU CM69

6, AUTHOR(S)
J. Yen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SSC San Diego
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER
TD 3100

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Space and Naval Warfare Systems Command
PMW 161
4301 Pacific Highway
San Diego, CA 92110

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This document describes the commercial off-the-shelf (COTS) security product evaluation process, defines the seven phases of the evaluation process, outlines the documentation requirements of the process, and discusses how the evaluation process fits into the overall evaluation framework. The evaluation process as described in this document is expected to be revised as the overall evaluation framework is developed. Appendix A contains additional information regarding Common Criteria and protection profiles and Appendix B contains additional details regarding the Information Assurance & Engineering Division (D87) formal inspection process.

14. SUBJECT TERMS
Mission Area: Command, Control, and Communications
COTS network software security
product evaluation process

15. NUMBER OF PAGES
62

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
SAME AS REPORT

21a. NAME OF RESPONSIBLE INDIVIDUAL J. Yen	21b. TELEPHONE *(include Area Code)* (619) 553–9404 e-mail: yen@spawar.navy.mil	21c. OFFICE SYMBOL D872

INITIAL DISTRIBUTION

D0012	Patent Counsel	(1)
D0271	Archive/Stock	(6)
D0274	Library	(2)
D027	M. E. Cathcart	(1)
D0271	D. Richter	(1)
D872	J. H. Yen	(10)
D0012	P. Lipovsky	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (4)

SSC San Diego Liaison Office
Arlington, VA 22202–4804

Center for Naval Analyses
Alexandria, VA 22302–0268

Navy Acquisition, Research and
Development Information Center
Arlington, VA 22202–3734

Government-Industry Data Exchange
Program Operations Center
Corona, CA 91718–8000